



## **- Supplement A -**



# **to the Navy Enterprise Application Deployment Guidance (NEADG)**

---

## **NMCI Release Development and Deployment Guide (NRDDG) v2.0**



**28 May 2004**

THE NMCI RELEASE DEVELOPMENT AND DEPLOYMENT GUIDE IS PUBLISHED FOR INFORMATION PURPOSES ONLY TO ILLUSTRATE APPLICATION PROCESSES AND INTERACTIONS. THE CONTENT OF THIS DOCUMENT SHALL NOT BE CONSIDERED CONTRACTUALLY BINDING. ALL ISSUES ASSOCIATED WITH THE NMCI CONTRACT N00024-00-D-6000 SHALL BE REFERRED TO THE PROCURING CONTRACTING OFFICER AT 619-524-7388.



DEPARTMENT OF THE NAVY  
DIRECTOR  
NAVY MARINE CORPS INTRANET OFFICE  
2231 CRYSTAL DRIVE  
CPK 3, SUITE 400  
ARLINGTON, VA 22202-3721

MEMORANDUM FOR DISTRIBUTION

Subj: NAVY MARINE CORPS INTRANET (NMCI) RELEASE DEVELOPMENT  
AND DEPLOYMENT GUIDE

Encl: 1) NMCI Release Development and Deployment Guide

1. The Department of the Navy is rapidly moving to a common computing and communications environment which will provide a modern, secure desktop and network infrastructure for the Navy and Marine Corps. The first step toward this goal is the Navy Marine Corps Intranet (NMCI) which will eventually support over 400,000 Navy and Marine Corps personnel. The move from independent, command networks to a single enterprise network is requiring many changes in the way the Department of the Navy manages information technology and software applications. We now need to have enterprise processes to use with our enterprise network. Many of these processes are being documented in the NMCI Information Advisories and NMCI Information Bulletins released by Commander, Naval Network Warfare Command in naval messages. Other NMCI enterprise processes will be documented in NMCI guides and publications.

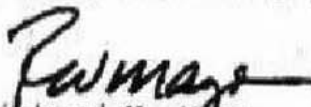
2. The Navy Enterprise Application Developer Guide (NEADG) provides general guidance to developers producing software for the Navy, particularly web-based applications. The NMCI Release Development and Deployment Guide (NRDDG), Supplement A to the NEADG, has been developed to specifically support application developers who are either maintaining existing applications or introducing new applications into the NMCI network. This guide defines the processes to be used by all participants in developing and deploying software on the NMCI. The NRDDG is not intended to replace or modify any Department of the Navy policy or acquisition guidance. The sole purpose of the NRDDG is to provide detailed NMCI business, technical, and process requirements that are consistent with established Department of the Navy policies.

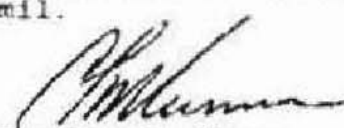
3. This is the first edition of the NMCI Release Development and Deployment Guide. The guide will continue to be refined and will be available on the Navy NMCI website (<http://nmci.navy.mil>), the Task Force Web website (<https://tfw.navy.mil>) and the NMCI-ISF website

Subj: NAVY MARINE CORPS INTRANET (NMCI) RELEASE DEVELOPMENT  
AND DEPLOYMENT GUIDE

(<http://www.nmci-ief.com/transition.html#Release>). Since the guide is intended to support software developers, we encourage comments and suggestions for incorporation into the next version. See the guide for information on how to submit your comments.

4. If any additional information is needed, please contact Mr. Peter Almazan (619) 606-2627, [peter.almazan@navy.mil](mailto:peter.almazan@navy.mil) or LCDR Joe Dundas (859) 537-8527, [joe.dundas@navy.mil](mailto:joe.dundas@navy.mil).

  
Richard W. Mayo  
Vice Admiral, U.S. Navy  
Commander, Naval Network  
Warfare Command  
Date Signed: 8/21/03

  
Charles L. Munns  
Rear Admiral, U.S. Navy  
Director, NMCI  
Date Signed: 13 Aug 2003

Distribution:

Immediate Office of Secretary  
(ASN (M&R), ASN (RD&A), ASN (I&E), ASN (PM&C), AAUSN,  
Dept of the Navy Staff Offices  
(OPA, JAG, OLA, CHINFO, NAVINSGEN, OGC) only  
CNO (N09, N09B, N093, N096, N1, N2, N3/5, N4, N6/N7, N8)  
CMC (ACMC)  
COMPAFLT  
COMLANTFLT  
COMUSNAVEUR  
CHNAVPERS  
COMSC  
COMUSNAVCENT  
COMNAVAIRSYS COM  
COMNAVSUPSYS COM  
COMNAVSEASYS COM  
COMSPAWARSYS COM  
COMNAVNETOPSCOM  
COMNAVFACENGCOM  
COMNAVSECGRU  
NETC  
BUMED  
NCTSI  
COMNAVDIST Washington  
USNA  
COMNAVSPCWARCOM

~~Subj: NAVY MARINE CORPS INTRANET (NMCI) RELEASE DEVELOPMENT  
AND DEPLOYMENT GUIDE~~

Distribution: (cont.)

NAVHISTCEN

COMNAVSAFECEN

ONI

NAVOBSY

NAVPGSCOL

COMNAVLEGSVCCOM

COMNAVMETOCCOM

COMNAVRESFOR

COMNAVSPACECOM

DIRSSP

FLDSUPPACT

OPNAVSUPPACT

PRESINSURV

NAVWARCOL

NAVSTKAIRWARCEN

ONR

MARCORSYSCOM

MARFORPAC

MARFORLANT

MARFORRES

MCCDC

## CHANGE HISTORY

The following Change History log contains a record of changes made to this document. Entries should be made in descending order, with most recent changes at the top of table.

<b>Published / Revised Date</b>	<b>Version # [ 0.XX for unpublished documents]</b>	<b>Author(s)</b>	<b>Section / Nature of Change</b>
28 May 2004	v2.0	NRDDG Working Group	Major revision and update
13 Nov 2003	v1.3	NRDDG Working Group	Major revision and update
15 Jul 2003	v1.2	NRDDG Working Group	Major revision and update
17 Mar 2003	v1.1	NRDDG Working Group	Review and revision
20 Dec 2002	DRAFT v1.1	NRDDG Working Group	Major revision and update
30 Sept 2002	DRAFT v1.0	Steven Baracosa in collaboration with others	Initial of version of revised guide taken from ARG and NEADG

### Document Properties

Owner: Director NMCI

Please send feedback on this version of the NRDDG in the suggested format below to:

NMCI PMO Developer Guidance Support  
[npmo-Legapps@navy.mil](mailto:npmo-Legapps@navy.mil)  
858-537-8249

Format:

<b>Paragraph #</b>	<b>Problem/Concern</b>	<b>Recommended Solution</b>

Your comments and recommendations to improve this guide are highly encouraged. As you review its contents consider these questions:

Does this guide give you what you need?  
Does this guide overly constrain you and how?

In your response please ensure that you clearly reference the paragraph being addressed, explain the problem or concern and provide a recommended solution.

## NRDDG v2.0 Summary of Changes

Each new version is date stamped with the date that the change was made to the respective document.

Section/Paragraph #	Revision
<a href="#">1.0</a> Introduction	Created a separate section for overview of the NMCI program and introduced Marine Corps content. Removed references to NMCI Product Evaluation Center (NPEC) and training.
<a href="#">2.0</a> Roles and Responsibilities	Established a separate Section 2.0, added Marine Corps content and updated Navy content: <ul style="list-style-type: none"> <li>• Updated Deputy DON CIO to include Marine Corps NMCI DAA.</li> <li>• Director NMCI</li> <li>• Designated Approval Authority (DAA)</li> <li>• Removed Navy Application Database Task Force (NADTF)</li> <li>• Updated NMCI PMO roles and responsibilities, including NSCM, QUEST, DMT, and CCS.</li> <li>• Introduced content for Marine Corps Network Operations Security Command (MCNOSC), Marine Corps Systems Command – Information Systems and Infrastructure (MCSC ISI), Program Manager NMCI Inspection/Test Instruction (ITI), and MCSC Enterprise Business Systems Support (EBSS).</li> </ul>
<a href="#">2.7</a> Command Responsibilities	Redefined terminology to include Navy and Marine Corps designations: <ul style="list-style-type: none"> <li>• Claimant to Command</li> <li>• Sponsoring Echelon II to Command.</li> <li>• Program of Record (POR) to Program of Record Program Manager (POR-PM)</li> <li>• Central Design Activity (CDA) to developer.</li> </ul>
<a href="#">3.0</a> NMCI Release Management Process (NRMP)	Made major changes and revisions, recommend reviewing in its entirety.
<a href="#">3.5.6</a> NMCI Application Business Rules	Added NMCI Post Transition Application Business Rules Decision Logic Table (DLT) and NMCI Site/Command Application Request Business Rules DLT
<a href="#">3.6</a> Requesting Release in the Post Transition Environment (RRPTE)	Revised process and included Service Request Management (SRM) for submission of Move, Add, Change (MAC) forms and Distribution CLINs.
<a href="#">4.0</a> Preparation and Analysis	Revised and updated existing information and added new requirements.
<a href="#">4.4</a> FAM Processing Summary	Revised process and added FAM status definitions.
<a href="#">4.12</a> NMCI Application Services	Updated services and CLIN information.
<a href="#">4.12.1</a> Service Request Management (SRM)	Added content for SRM process and submission of MAC, Certification CLIN, and Distribution CLIN.
<a href="#">5.0</a> Design and Development	Revised and updated existing information.
<a href="#">6.0</a> NMCI Release Deployment Process (NRDP)	Made significant process changes and added process content. <ul style="list-style-type: none"> <li>• Aligned Release Deployment Plan (RDP) with processes and added greater detail on the information contained in RDP.</li> <li>• Updated and streamlines Request to Deploy (RTD) form and</li> </ul>

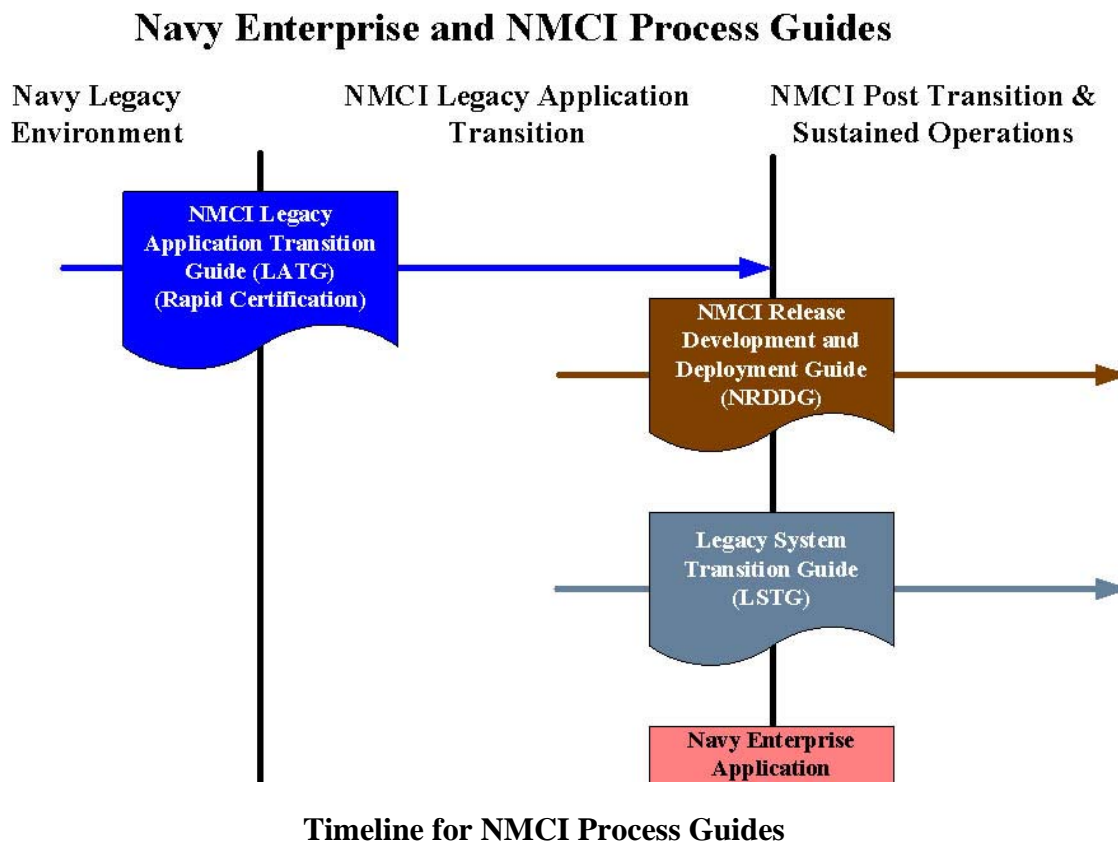
Section/Paragraph #	Revision
	<p>process.</p> <ul style="list-style-type: none"> <li>• Introduced RTD Cancellation Process.</li> <li>• Process and content changes to Preparation, Collection and Submission, Packaging and Certification, Accreditation and Risk Mitigation, Release Deployment Documentation, and Enterprise Change Control Board (ECCB), Application Release Deployment Readiness Activity (ARDRA), and ARDRA/Pilot Test.</li> </ul>
<a href="#">6.1</a> Release Deployment Plan (RDP)	RDP form and process streamlined to contain only essential information necessary to complete packaging, testing, certification, and deployment.
<a href="#">6.2</a> Request to Deploy (RTD)	RTD form and process streamlined to contain only essential information necessary to complete packaging, testing, certification, and deployment.
<a href="#">6.3</a> Release Approval, Prioritization, and Scheduling	Process revised to comply with changes made to the RTD.
<a href="#">6.3.3</a> RTD Cancellation Process	Added new NNWC RTD cancellation process.
<a href="#">6.6.2</a> Precertification	Introduced Navy and Marine Corps application Precertification activities.
Previous Section 6.0 Conclusion	Removed section. Moved content into Introduction.
<a href="#">Appendix A</a> Glossary of Acronyms and Terms	<p>Updated definitions:</p> <ul style="list-style-type: none"> <li>• Changed CDA to developer to include Marine Corps terminology.</li> <li>• Changed definition for ISF.</li> <li>• Removed NATF.</li> <li>• Changed NETWARCOM to NNWC.</li> <li>• Added definitions for RDP, RRPTE, and RTD.</li> </ul>
<a href="#">Appendix B</a> Hyperlinks, Navy Messages, and Documents	Renamed appendix to reflect the content. Updated and added to the hyperlink listings.
<a href="#">Appendix C</a> Points of Contact	Updated contacts.
<a href="#">Appendix F</a> Developer Checklist	Major revision.
<a href="#">Appendix G</a> Release Deployment Plan (RDP)	Updated.
<a href="#">Appendix H</a> Navy Functional Area Manager (FAM)	Updated FAM list to include Marine Corps content.
<a href="#">Appendix I</a> Examples and Templates	Deleted Help Desk Templates
<a href="#">Appendix J</a> Request to Deploy (RTD)	Updated.
Previous Appendix K Classified Release Deployment Process	Removed appendix. Moved classified material into pertinent paragraphs of Section 6.0.

Section/Paragraph #	Revision
<a href="#">Appendix K</a> Advanced Publisher .msi Packaging	Added.



## NAVY ENTERPRISE AND NMCI PROCESS GUIDES

The graphic below illustrates how the NMCI Process Guides are used throughout the lifecycle of the NMCI program. The following paragraphs briefly summarize each guide listed within the timeline.



### Legacy Application Transition Guide (LATG)

The LATG presents a complete baseline overview of the Legacy Applications Rapid Certification Phase of the Legacy Applications Transition Process. It is for NMCI customers involved with transition activities. Electronic Data Systems (EDS) and Government program management personnel worked in close cooperation to design the processes, procedures, and policies described in the LATG. The LATG describes in detail the roles and responsibilities of those organizations and positions involved in transitioning Legacy Applications through the Rapid Certification Phase.

### Navy Enterprise Application Development Guidance (NEADG)

The purpose of the NEADG is to provide detailed information and direction to developers tasked with migrating applications, content, and services into the Department of the Navy (DON) Enterprise Information Technology (IT) Environment. This effort seeks to align current software development community practices within the Navy and Marine Corps with the best practice vision embraced by the DON and the Department of Defense (DoD). Their vision is a web-enabled enterprise application that is extensible, scalable, and open in its use of current standards and leading edge technologies. Additionally, the NEADG seeks to present guidance information in a way that is easily searchable manually and by

machine and that adds value to information consumers by aligning the guidance to their specific activities and roles. This is accomplished by mapping constituent guide content to searchable metadata categories to allow distinct renderings or views of the original data. The web-based platform enables the collection and packaging of content from other guides focused on the overall purpose of guiding developers in transitioning of applications toward the DON Enterprise IT Environment.

### **NMCI Release Development and Deployment Guide (NRDDG)**

The NRDDG is a consolidated source of information, guidance, and direction to developers and application owners who build and/or modify applications, as well as the acquirers of applications intended for use within NMCI. As a supplement to the NEADG, the NRDDG is written to support the developer in the development and deployment of releases to operate within the Navy Marine Corps Intranet (NMCI). For web-based application guidance, the user should refer to the NEADG, the Task Force Web (TFW), and the Navy Enterprise Portal (NEP). NRDDG fulfills an intermediary requirement in bridging the gap between present application development cycles underway by the developers and the target state of web-enablement of all Navy Enterprise applications under the TFW initiative.

### **Legacy Systems Transition Guide (LSTG)**

The LSTG provides both an approach and the associated processes to successfully transition systems from legacy environments to the NMCI environment while maintaining or improving system performance and availability. The LSTG provides the site representative, the developer, and the Program of Record-Program Manager (POR-PM) with the unique processes, tools/templates, and documentation guidelines to plan and execute the transition of their respective systems to the NMCI environment.

## TABLE OF CONTENTS

	Page
<b>1.0 INTRODUCTION .....</b>	<b>1-1</b>
1.1 Navy Marine Corps Intranet (NMCI) Overview.....	1-1
1.2 Marine Corps Community of Interest (COI).....	1-2
1.3 Legacy Applications .....	1-2
1.4 NMCI Release Development and Deployment Guide (NRDDG) Overview .....	1-2
1.4.1 NMCI Release Management Process (NRMP).....	1-3
1.4.2 NMCI Release Deployment Process (NRDP) .....	1-4
<b>2.0 ROLES AND RESPONSIBILITIES.....</b>	<b>2-1</b>
2.1 Department of the Navy Chief Information Officer (DON CIO) .....	2-1
2.1.1 Deputy DON CIO (Navy).....	2-1
2.1.2 Deputy DON CIO (Marine Corps) .....	2-3
2.1.3 Director NMCI.....	2-4
2.1.4 Functional Area Manager (FAM) .....	2-4
2.1.5 Functional Data Manager (FDM) .....	2-6
2.2 Designated Approval Authority (DAA).....	2-6
2.2.1 Navy NMCI DAA.....	2-6
2.2.2 Marine Corps NMCI DAA .....	2-7
2.3 Commander Naval Network Warfare Command (NNWC).....	2-7
2.3.1 NMCI Release Prioritization Manager (NRPM) .....	2-8
2.3.2 NMCI Release Scheduling Manager (NRSMP) .....	2-8
2.4 Marine Corps Network Operations Security Command (MCNOSC).....	2-8
2.5 Navy NMCI Program Management Office (PMO) .....	2-9
2.5.1 Enterprise Application Group for Legacy and Emerging (EAGLE) .....	2-9
2.6 Marine Corps NMCI PMO .....	2-14
2.6.1 Marine Corps Systems Command – Information Systems and Infrastructure (MCSC ISI).....	2-14
2.6.2 Program Manager NMCI Inspection/Test Instruction (ITI) .....	2-14
2.6.3 Program Manager Enterprise Business Systems Support (EBSS).....	2-14
2.7 Command Responsibilities .....	2-15
2.7.1 Sponsoring Command.....	2-15
2.7.2 Program of Record Program Manager ((POR-PM) .....	2-16
2.7.3 Developer.....	2-16
2.8 Electronic Data Systems (EDS) .....	2-16
2.8.1 Applications Lab.....	2-17
2.8.2 Site Manager (SM).....	2-17
2.8.3 Enterprise Change Control Board (ECCB).....	2-17
2.8.4 Application Project Manager (APM).....	2-17
<b>3.0 NMCI RELEASE MANAGEMENT PROCESS (NRMP).....</b>	<b>3-1</b>
3.1 Approval .....	3-2
3.1.1 Requirement Determination.....	3-2
3.1.2 FAM Approval.....	3-2
3.2 Development.....	3-3
3.3 Deployment.....	3-3

## TABLE OF CONTENTS, CONT.

	Page
3.4 Sustained Operations .....	3-3
3.5 Software Definitions and Processing Requirements .....	3-3
3.5.1 Client/Desktop/Standalone (Simple) Applications .....	3-3
3.5.2 Web Applications .....	3-3
3.5.3 Server-Based Applications .....	3-4
3.5.4 Client/Server Application .....	3-4
3.5.5 Application Decision Logic Table (DLT).....	3-4
3.5.6 NMCI Application Business Rules.....	3-10
3.6 Requesting Release in the Post Transition Environment (RRPTE) .....	3-14
3.6.1 Requirement Determination.....	3-16
3.6.2 Review Contract Line Item Number (CLIN) 0023 Catalog of Applications.....	3-16
3.6.3 Optional User Capabilities Catalog CLIN 0023 .....	3-17
3.6.4 Solution Deployed in NMCI.....	3-17
3.6.5 Contract Technical Representative (CTR) and Activity Contract Technical Representative (ACTR) Approval .....	3-17
3.6.6 Add Application to Rationalized List .....	3-17
3.6.7 Complete an Service Request Management (SRM) [Move, Add, Change (MAC)] Form or Distribution CLIN.....	3-17
3.6.8 Complete Application Mapping.....	3-18
3.6.9 License Requirement .....	3-18
3.6.10 License Verification.....	3-18
3.6.11 Submit Completed SRM (MAC) Form or Distribution CLIN.....	3-18
3.6.12 Perform Limited Deployment Evaluation.....	3-18
3.6.13 Coordinate Deployment.....	3-19
3.6.14 Deploy Release to Sites/Users .....	3-19
<b>4.0 PREPARATION AND ANALYSIS .....</b>	<b>4-1</b>
4.1 Data Collection and Assessment.....	4-1
4.2 Enterprise Rationalization.....	4-1
4.3 Department of the Navy Application Database Management System (DADMS).....	4-1
4.4 FAM Process Summary .....	4-2
4.4.1 Failed Status for FAM Disapproved Applications.....	4-2
4.5 NMCI Application Ruleset .....	4-2
4.6 FAM Application Waiver Process .....	4-2
4.6.1 How to Waiver an Application .....	4-3
4.7 Certification and Accreditation (C&A) .....	4-3
4.7.1 Purpose .....	4-4
4.7.2 DITSCAP Application Manual Objectives.....	4-4
4.7.3 Application and Scope .....	4-5
4.7.4 NMCI DAA Policy for Certification and Accreditation of Applications on NMCI4-5	
4.8 Information Assurance (IA).....	4-5
4.9 Security .....	4-6
4.9.1 Boundary Protection .....	4-6
4.9.2 NMCI Public Key Infrastructure & Directory System .....	4-7
4.9.3 Boundary 1 (B1) Conditionally Allowed Ports .....	4-7
4.9.4 Active Directory (AD).....	4-7

## TABLE OF CONTENTS, CONT.

	Page
4.9.5 Security Objects: Group Policy Objects (GPOs) .....	4-8
4.9.6 Security Management .....	4-8
4.9.7 Firewall Policies .....	4-8
4.9.8 Desktop GPO Implementation.....	4-8
4.9.9 File and Registry Permission .....	4-8
4.10 Information Access & System Services .....	4-9
4.10.1 CLIN .....	4-9
4.10.2 File and Print Services .....	4-9
4.10.3 Print Services .....	4-10
4.10.4 File Storage Services .....	4-10
4.10.5 File Sharing.....	4-10
4.10.6 Personal Storage .....	4-11
4.10.7 Shared Storage .....	4-11
4.10.8 File Share Naming Conventions .....	4-11
4.10.9 Printer Naming Format .....	4-11
4.10.10 Messaging and Collaboration .....	4-12
4.11 Platforms .....	4-13
4.11.1 Client Seat.....	4-13
4.11.2 Science and Technology (S&T) Seat.....	4-13
4.12 NMCI Application Services.....	4-15
4.12.1 Service Request Management (SRM).....	4-16
4.12.2 Gold Disk.....	4-17
4.12.3 NMCI Server Connectivity CLIN 0027.....	4-17
4.12.4 NMCI Legacy Systems Support CLIN 0029 .....	4-17
4.13 Components .....	4-17
4.14 Directory and Registry Permissions.....	4-17
4.15 Browsers .....	4-18
4.15.1 Microsoft Internet Explorer Version 5.0 or Greater .....	4-18
4.15.2 Netscape Communicator 4.76.....	4-18
4.15.3 Browser Security.....	4-18
4.16 Emulation.....	4-18
4.16.1 Terminal Services .....	4-18
4.16.2 Product Supported.....	4-18
4.17 Integrated Solution Framework (ISF) Tools Database Registration.....	4-18
4.17.1 ISF Tools Database Description .....	4-19
4.18 NMCI Help Desk Support .....	4-19
4.18.1 Level 1 NMCI Help Desk Support .....	4-19
4.18.2 Level 2 and Higher NMCI Help Desk Support .....	4-20
<b>5.0 DESIGN AND DEVELOPMENT .....</b>	<b>5-1</b>
5.1 Standards/Programming Practices .....	5-1
5.1.1 Microsoft Development Standards .....	5-1
5.1.2 Programming Guidelines .....	5-1
5.2 Programming Standards for a Terminal Server Platform .....	5-2
5.3 User Interface Specifications .....	5-2
5.4 Group Policy Object (GPO).....	5-2

## TABLE OF CONTENTS, CONT.

	Page
5.5	Application Testing Guidelines for Developers.....5-3
5.5.1	Do's.....5-3
5.5.2	Don'ts .....5-5
5.5.3	Recommendations.....5-6
5.6	NMCI Interfaces .....5-7
5.6.1	Windows 2000 Desktop Application Interface Specification.....5-7
5.6.2	Microsoft Windows 2000 Server Interface Specification.....5-7
5.6.3	Mobile Code .....5-8
5.7	Boundary/Network Interface Specifications.....5-8
5.7.1	Transport Boundary (TB) .....5-8
5.7.2	Boundary 1 (B1) .....5-8
5.7.3	Boundary 2 (B2) .....5-9
5.7.4	Boundary 3 (B3) .....5-9
5.7.5	Boundary 4 (B4) .....5-9
5.8	Network-Related APIs Other Than Standard Windows 2000 ADSI.....5-9
5.9	NMCI Lockdown Policy.....5-9
5.10	Software Installation .....5-9
5.11	Screen Saver .....5-9
5.12	Terminal Service.....5-9
5.13	Testing Considerations .....5-10
<b>6.0</b>	<b>NMCI RELEASE DEPLOYMENT PROCESS (NRDP).....6-1</b>
6.1	Release Deployment Plan (RDP).....6-3
6.2	Request to Deploy (RTD) .....6-4
6.2.1	Quarantine/Kiosk Solutions [New (Emerging)] .....6-4
6.2.2	Quarantine/Kiosk Solutions (Using an Existing Radia Application).....6-4
6.2.3	Type of Release .....6-4
6.3	Release Approval, Prioritization, and Scheduling .....6-6
6.3.1	NMCI RTD Prioritization and Scheduling (Planned Release) .....6-6
6.3.2	NMCI RTD Prioritization and Scheduling (Unplanned Release).....6-8
6.3.3	RTD Cancellation Process.....6-10
6.4	Timeline for NRDP.....6-11
6.4.1	Notional Processing Timeline for Planned Releases .....6-11
6.4.2	Notional Processing Timeline for Unplanned Releases.....6-11
6.4.3	Submission.....6-12
6.4.4	Receipt, Audit, Packaging, and Certification.....6-12
6.4.5	Accreditation and Risk Mitigation (A&RM).....6-13
6.4.6	Enterprise Change Control Board (ECCB).....6-13
6.4.7	Application Release Deployment Readiness Activity (ARDRA).....6-13
6.4.8	Release Push/Deployment to the Desktop .....6-13
6.5	Preparation.....6-13
6.5.1	Begin Application Mapping Plan .....6-14
6.5.2	Develop ARDRA/Pilot Test Plan .....6-14
6.5.3	Gather Existing Precertification Data, Systems Architecture Connectivity Diagrams, ATO/IATO, & DITSCAP Documentation.....6-14
6.5.4	Precertification.....6-15

## TABLE OF CONTENTS, CONT.

	<b>Page</b>
6.5.5 Begin New or Updated DITSCAP Documentation .....	6-18
6.5.6 Develop RDP .....	6-18
6.6 Collection and Submission .....	6-19
6.6.1 Generate CDA Request for Services (RFS)/USMC RFS .....	6-19
6.6.2 Application Submission Packet .....	6-20
6.6.3 Update Release Deployment Plan.....	6-21
6.6.4 Finalize New or Updated DITSCAP Documentation .....	6-23
6.6.5 Submit RDP .....	6-23
6.7 Packaging and Certification.....	6-24
6.7.1 Audit the Application Submission Packet .....	6-25
6.7.2 Radia Packaging .....	6-25
6.7.3 Lab and Developer Usability Test .....	6-26
6.7.4 Gold Disk Testing .....	6-27
6.7.5 Quick Fix .....	6-27
6.7.6 Final Certification Lab Process.....	6-27
6.8 Accreditation and Risk Mitigation.....	6-27
6.9 Release Deployment Documentation.....	6-28
6.10 ECCB .....	6-30
6.11 Predeployment .....	6-31
6.12 Application Release Deployment Readiness Activity (ARDRA).....	6-32
6.12.1 ARDRA/Pilot Test Plan.....	6-33
6.13 ARDRA/Pilot Test.....	6-33
6.14 Deployment.....	6-35

## **LIST OF APPENDICES**

**APPENDIX A: GLOSSARY OF ACRONYMS AND TERMS**

**APPENDIX B: REFERENCES**

**APPENDIX C: POINTS OF CONTACT**

**APPENDIX D: NMCI APPLICATION RULESET (REVISED)**

**APPENDIX E: FACTORS AND ISSUES FOR APPLICATION MIGRATION**

**APPENDIX F: DEVELOPER CHECKLIST**

**APPENDIX G: RELEASE DEPLOYMENT PLAN**

**APPENDIX H: NAVY FUNCTIONAL AREA MANAGER (FAM) LIST**

**APPENDIX I: EXAMPLES AND TEMPLATES**

**APPENDIX J: REQUEST TO REPLOY (RTD)**

**APPENDIX K: ADVANCED PUBLISHER .MSI PACKAGING**



## LIST OF FIGURES

	<b>Page</b>
Figure 1-1 Architecture Management Framework.....	1-1
Figure 2-1 DON CIO Organization Chart.....	2-1
Figure 3-1 NMCI Release Management Process .....	3-2
Figure 3-2 RRPTE .....	3-15
Figure 3-3 RRPTE Legend .....	3-16
Figure 4-1 Network Boundaries.....	4-6
Figure 6-1 NRDP .....	6-2
Figure 6-2 NRDP Legend .....	6-3
Figure 6-3 NMCI RTD Prioritization and Scheduling (Planned Release).....	6-6
Figure 6-4 NMCI RTD Prioritization and Scheduling (Unplanned Release) .....	6-9
Figure 6-5 Timeline for NMCI Application Release Deployment Process (Planned Release) .....	6-11
Figure 6-6 Timeline for NMCI Application Release Deployment Process (Unplanned Release).....	6-12
Figure 6-7 Preparation Process .....	6-14
Figure 6-8 Precertification Process.....	6-16
Figure 6-9 Collection and Submission Process.....	6-19
Figure 6-10 Packaging and Certification .....	6-24
Figure 6-11 Lab and Developer Usability Test.....	6-26
Figure 6-12 Accreditation and Risk Mitigation .....	6-28
Figure 6-13 Release Deployment Documentation .....	6-29
Figure 6-14 Enterprise Change Control Board (ECCB) .....	6-30
Figure 6-15 Predeployment Process .....	6-31
Figure 6-16 Application Release Deployment Readiness Activity (ARDRA) .....	6-32
Figure 6-17 ARDRA/Pilot Test Plan .....	6-34

## LIST OF TABLES

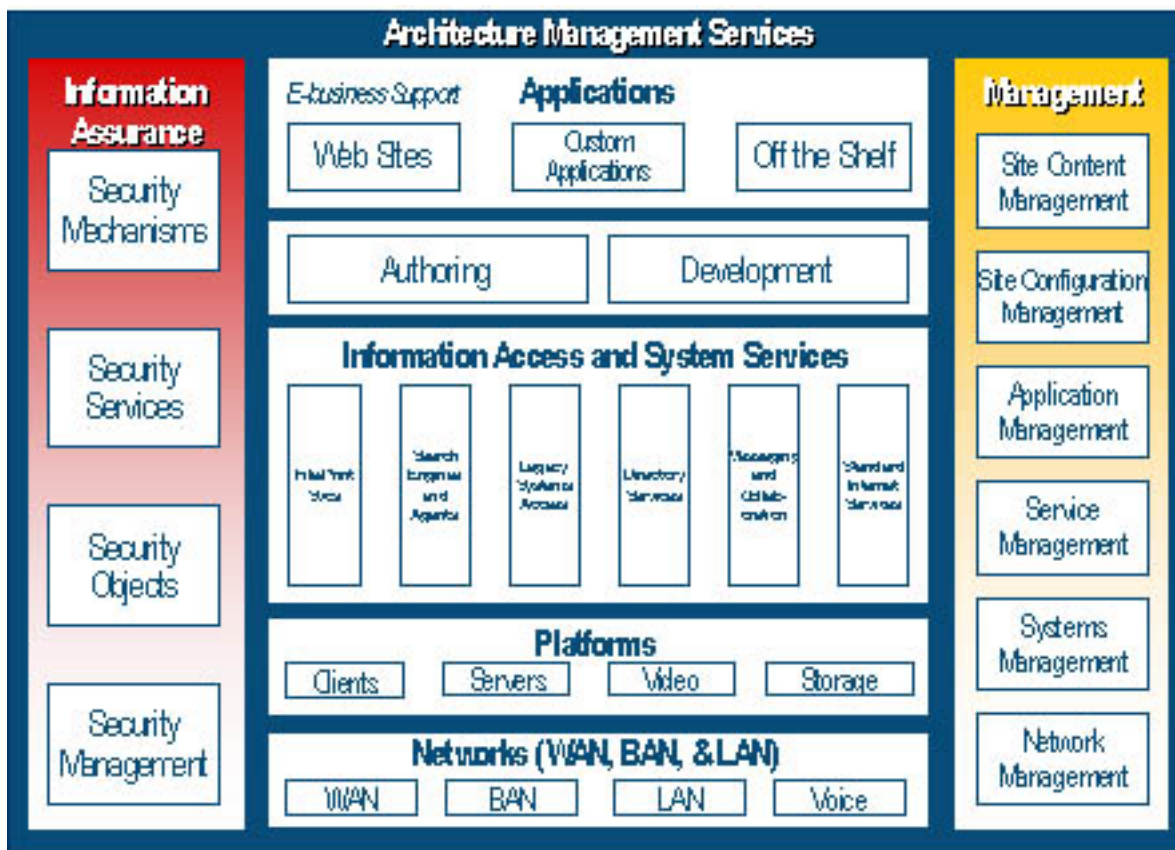
	<b>Page</b>
Table 3-1 NMCI Application DLT .....	3-5
Table 3-2. NMCI Post Transition Application Business Rules DLT.....	3-10
Table 3-3. NMCI Site/Command Application Request Business Rules DLT .....	3-12
Table 4-1 Available Drive Letters and Backup Routines .....	4-10
Table 4-2 File Share Naming Conventions.....	4-11
Table 4-3 Printer Naming Format .....	4-12

## 1.0 INTRODUCTION

### 1.1 NAVY MARINE CORPS INTRANET (NMCI) OVERVIEW

The NMCI is an Information Technology (IT) initiative and procurement strategy to provide secure, seamless, global end-to-end connectivity for Navy and Marine Corps Warfighting and business functions. When completed, NMCI will consolidate Navy and Marine Corps computer networks into a single, secure, enterprise-wide managed service for voice, video, and data information exchange.

Figure 1-1 depicts a detailed overall design diagram of the Navy NMCI architecture. It shows the logical and physical architectures. It represents the architecture by subcomponent and includes conceptual issues and items relating to security, management functionality, and deployment.



**Figure 1-1 Architecture Management Framework**

NMCI program represents a major IT initiative to consolidate a multitude of Navy and Marine Corps base- and installation-specific computer networks into a single intranet network for both classified and unclassified applications. This initiative draws heavily on “industry best practices and procedures.” The Navy and Marine Corps have been challenged to adapt these industry procedures to the operational and administrative requirements of their services.

As part of the initial NMCI seat deployment process, the Navy and Marine Corps undertook efforts to identify and minimize the number of applications on Navy and Marine Corps administrative networks.

The intent was to provide a commonality of function and to minimize training requirements. The rollout then installed the identified legacy applications onto the new NMCI.

Legacy applications are identified as those previously running on the Navy various administrative networks. For the context of this guide, a release includes the introduction of a new (emerging) application or a change to an existing application. A change can be identified as a software patch, fix, update, upgrade, modification, revision, or new version to an existing application that operates within NMCI.

## **1.2 MARINE CORPS COMMUNITY OF INTEREST (COI)**

Some COIs (e.g., the Marine Corps) require the NMCI architecture to provide a separate enclave that rides the overarching NMCI. This COI enclave allows security management and operational direction and is separated from NMCI at large through Boundary 2 (B2) firewall suites. These B2 firewalls enable implementation of a security domain, similar to establishing a service-wide COI and support implementation of unique security requirements. B2 firewall suites providing this function mirror the NMCI solution for meeting Boundary 1 (B1) security requirements.

*Bottom line: The Marine Corps will retain autonomous security management and operational control over Marine Corps Enterprise Network (MCEN), to include the NMCI.*

## **1.3 LEGACY APPLICATIONS**

As defined by the NMCI contract, a legacy application is “An existing customer software application that is not included in the NMCI standard seat services or the Contract Line Item Number (CLIN) 0023 catalog.” Applications are in use today by people performing the mission or business of the DON. Legacy applications are NOT part of the standard seat services (also known as Gold Disk) provided by EDS.

The NMCI Legacy Application Transition Guide (LATG) provides the detailed guidance to transition Department of the Navy (DON) legacy applications into the NMCI environment. The transition of legacy applications is beyond the scope of the NMCI Release Development and Deployment Guide (NRDDG).

For more information: [http://www.nmci-isf.com/legacy\\_applications\\_transition\\_guide.pdf](http://www.nmci-isf.com/legacy_applications_transition_guide.pdf).

## **1.4 NMCI RELEASE DEVELOPMENT AND DEPLOYMENT GUIDE (NRDDG) OVERVIEW**

The NRDDG is a collaborative effort between the Navy and Marine Corps (the customers) and Electronic Data Systems (EDS) (the contractor). The Commander Naval Network Warfare Command and the Director NMCI have certified the NRDDG as the authoritative guide to provide detailed NMCI business, technical, and process requirements that are consistent with established DON policies. The NRDDG provides policy, guidance, and process information to achieve the following stated contract goals:

- Consolidate and provide NMCI-specific enterprise application development and deployment guidance for the Navy and Marine Corps in one comprehensive document.

- Eliminate the confusion of multiple documents that address only portions of the release development and deployment process for NMCI applications.
- Provide detailed information and guidance to application developers interested in migrating content, introducing new (emerging) applications, quarantine/kiosk remediation solutions, or changing existing applications within NMCI.
- Reduce the time and cost of developing, modifying, and deploying releases.
- Support required activities within the overall NMCI Release Management Process (NRMP).
- Provide guidance for NMCI application maintenance and implementation during the interim period until the Navy Enterprise Portal (NEP) initiative under Task Force Web (TFW) is complete. For guidance on web-based applications, refer to the Navy Enterprise Application Development Guidance (NEADG), the TFW, and the NEP.
- Support developers who develop and deploy releases to operate within NMCI as a supplement to the NEADG.
- Act as a work in progress with enhancements inserted as required to support the current state of NMCI implementation.
- Eliminate the proliferation of unnecessary, redundant, and excess applications inherent in legacy systems.

The NRDDG contains two major processes to support the goals and objectives of NMCI in the post transition environment:

- NMCI Release Management Process (NRMP)
- NMCI Release Deployment Process (NRDP)

#### **1.4.1 NMCI Release Management Process (NRMP)**

The NRMP provides a structured approach to software application management across the enterprise and enforces the necessary management and discipline needed to maintain and control enterprise size, configuration, and security of Navy and Marine Corps applications.

The purpose of the NRMP is to eliminate the proliferation of unnecessary, redundant, and excess applications that are inherent in the legacy system today. As part of the NRMP, all releases are subject to an executive review and approval for appropriateness within the enterprise. The NRMP has many steps that must be completed prior to approving the development and subsequent deployment of a release within NMCI. New (emerging) or updated applications are part of overall Navy and Marine Corps Enterprise application management and are reviewed in accordance with strict guidelines contained in the NRMP.

Refer to Section 3.0 for detailed information on the NRMP.

### **1.4.2 NMCI Release Deployment Process (NRDP)**

The NRDP consists of a set of subordinate processes or tasks that a developer or Command must follow in order to successfully deploy within the NMCI environment:

- Preparation
- Precertification
- Collection and Submission
- Packaging and Certification
- Accreditation and Risk Mitigation
- ECCB
- Predeployment
- Application Release Deployment Readiness Activity (ARDRA)
- Deployment

Refer to Section 6.0 for detailed information on the NRDP.

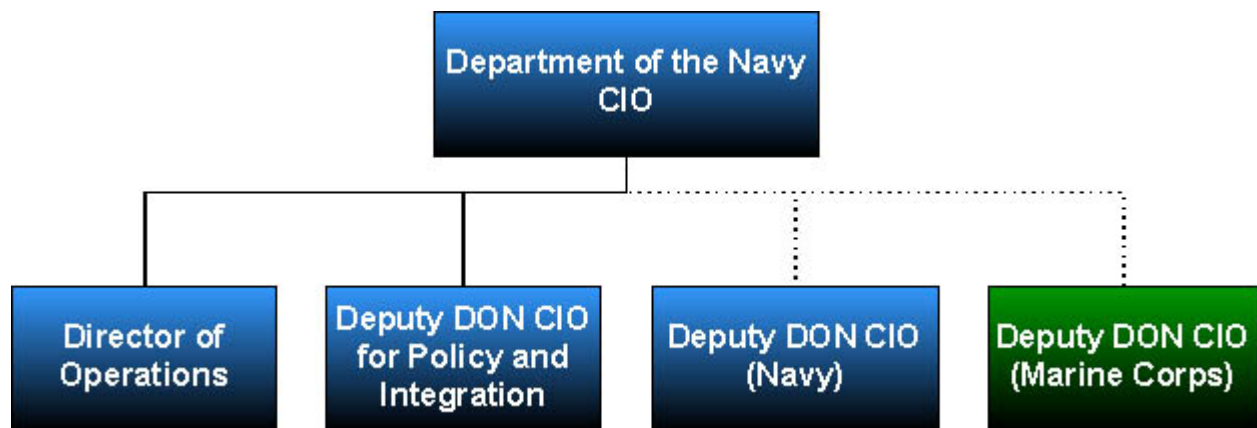
## 2.0 ROLES AND RESPONSIBILITIES

This section lists the organizations and individuals responsible for the execution and day-to-day management of NMCI. This section provides detailed descriptions of their roles and responsibilities in supporting the processes outlined in this guide.

### 2.1 DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER (DON CIO)

The DON CIO is organized to align and integrate Information Technology/Information Management (IT/IM) programs across the Navy and Marine Corps and to focus department-wide IT/IM efforts on warfighter priorities. Overall leadership responsibility is vested in the CIO, supported by the Deputy DON CIO (Navy) and Deputy DON CIO (Marine Corps). The Deputy DON CIO for Policy and Integration directs the operations of the DON CIO Functional Teams. The teams advance the goals and objectives of the DON IT/IM Strategic Plan.

Figure 2-1 depicts the senior executive staff positions of the DON CIO organization. The Deputy DON CIO (Navy) and Deputy DON CIO (Marine Corps) are responsible for implementing DON IT/IM programs and policies at the service level.



**Figure 2-1 DON CIO Organization Chart**

#### 2.1.1 Deputy DON CIO (Navy)

The Deputy DON CIO (Navy) is responsible for the following:

- Bring operational IT/IM requirements into alignment with Navy functionality capabilities using developed and established processes and procedures.
- Advise and assist the Chief of Naval Operations (CNO) in achieving network-centric operational capabilities by managing robust global and local networks, employing proven-successful business practices, and integrating IT/IM as it applies to warfighters at sea and the supporting shore establishment.
- Oversee the integration of dispersed sea-based and joint command and control architectures.
- Champion the incorporation of significant industry improvements in IT, in such areas as supply chain and enterprise resource management, into the Navy enterprise.

- Lead the development of strategic plans and implementation strategies for managing global Navy enterprise IT solutions across the Navy.
- Receive requirements from and provide policies and procedures to Commander, Naval Network Warfare Command (NNWC), who is responsible for their implementation.
- Reduce legacy applications and databases in order to support the rapid transition to NMCI.
- Work with and provide guidance to the Functional Area Managers (FAMs), who are ultimately responsible for determining the suite of approved applications and databases used in their business area in order to accomplish the mission.
- Work with Program Executive Office for Information Technology (PEO-IT) to determine the policies and processes for procuring enterprise licenses for applications that have a significant user base across the Navy enterprise, leveraging the capabilities of the NMCI to enhance operations and communications within the Navy.
- Ensure that IT/IM requirements are consistent and compliant with overall Navy/DoD joint architectures and investment decisions.
- Work closely with the DON and the Deputy DON CIO (Marine Corps) to manage “information” and “knowledge” as key strategic resources in order to satisfy Fleet information requirements.
- Oversee the development and implementation of systems, policies, and processes to ensure the integrity, availability, authentication, and safeguarding of Navy information and information display, processing, and storage systems.
- Ensure Navy compliance with evolving national security Information Assurance (IA) policies through the acquisition and implementation of approved IT/IM products.
- Establish, manage, and enforce IT/IM configuration standards for hardware, software, and network connectivity.
- Oversee the development of an enterprise management process for IT/IM configuration control.
- Provide Navy leadership in support of DoD and DON CIO efforts to develop, maintain, implement, and evolve DoD Joint Information Architectures.
- Serve as the Navy lead point of contact (POC) for interaction and coordination with other Service, Joint, DoD, and interagency CIOs for implementing the Global Information Grid (GIG) enterprise solutions.
- Develop, coordinate, and ensure compliance with the Navy IT/IM Plan that serves as a key input to the DON IT/IM Strategic Plan. (The term “information technology” includes “national security systems,” as defined in the Clinger-Cohen Act of 1996.)
- Advise the CNO and other senior leadership on all IT/IM-related issues. Key to this function is close coordination and frequent liaison with DON and U.S. Marine Corps CIOs, the Fleet Commanders, Systems Commanders, Commander NNWC, and other Major Claimant CIOs.
- Support DoD and DON CIO efforts to promote effective and efficient design and operation of IM processes throughout the global Navy enterprise.

- Review and critique all Navy IT/IM Support Plans [Command, Control, Communications, Computers, and Intelligence Support Plans (C4ISPs)]. These are prepared and updated at each acquisition milestone in accordance with DoD 5000-series directives, to verify compliance with DoD Joint Technical Architectures and to ensure interoperability, compatibility, and integration with other Joint Warfighting and support systems.
- Oversee the implementation of a Navy-wide IT/IM systems-of-systems testing program to ensure continued interoperability.
- Develop and implement knowledge management strategies that facilitate the improved creation and sharing of knowledge. Knowledge management involves delivering the right information to the right decision-maker at the right time to create the right conditions for new knowledge. It enables more effective and agile decision-making, resulting in greatly improved mission performance.
- Promote results-based performance measures and best practices to improve mission performance and optimize the return on investment for IT/IM.

### **2.1.2 Deputy DON CIO (Marine Corps)**

The Deputy DON CIO (Marine Corps) is responsible for the following:

- Plan, direct, coordinate, and oversee all IT Marine Air Ground Task Force (MAGTF) functions.
- Provide strategic direction to enable the effective and efficient application, moderation, functional integration, acquisition, and management of all IT resources.
- Serve as the senior executive for Marine Corps IT.
- Formulate and publish Marine Corps IT strategy, goals, roadmaps, and objectives.
- Define and issue IT standards and policies consistent with the DoD, DON, and Joint Service mandates.
- Establish the Information Technology Steering Group (ITSG)
- Develop and maintain the Marine Corps Enterprise Information Technology Architecture (EITA)
- Act as the controlling authority for all Marine Corps network and networking activity.
- Act as the Designated Approving Authority (DAA) for the MCEN.
- Evaluate and approve/disapprove the connection of any application to the MCEN.
- Evaluate and confirm compliance of IT pilots and programs to the EITA.
- Prepare policies/orders for processing Marine Corps C4ISPs.
- Confirm that each program has an IA strategy that is compliant with DoD, DON, Marine Corps, and Joint Service policies and standards.
- Serve as IT funding coordinator.



- Develop and manage an integrated Enterprise portfolio of software application ensuring all new development complies with the EITA.

### **2.1.2.1 NMCI-Specific Functions**

The NMCI-specific functions include the following:

- Serve as the Marine Corps sponsor for NMCI.
- Oversee the Functional Program.
- Chair Marine Corps NMCI Transition C2 Operation Cell (CCOC).
- Cochair the NMCI Stakeholders' Council.
- Communicate Marine Corps NMCI policy and requirements.
- Serve as the Marine Corps Decision Authority on NMCI requirements and policy issues.
- Serve as the NMCI subject matter expert (SME) and web content manager in the areas of policy and requirements.

### **2.1.2.2 NMCI Roles and Responsibilities**

The NMCI-specific responsibilities include the following:

- Develop Marine Corps NMCI policy under the guidance/approval of the Marine Corps command, control, communications, computers (C4)/DON CIO.
- Oversee dissemination and implementation of policy for the Marine Corps COI within the NMCI.
- Oversee Marine Corps Network Operations Security Command (MCNOSC) and Computer Network Defense, reporting directly to Headquarters, Marine Corps (HQMC) C4.
- Cochair the NMCI Stakeholders' Council under NMCI Executive Council (Marine Corps, Navy, and DON CIO). (Membership: Major Marine Corps Commands and Navy Activities)

### **2.1.3 Director NMCI**

The Director NMCI manages the acquisition of NMCI under the Assistant Secretary of the Navy for Research Development and Acquisition (ASN RDA) and provides additional acquisition guidance to the Navy and Marine Corps NMCI Program Managers within policy constraints.

### **2.1.4 Functional Area Manager (FAM)**

The Under Secretary of the Navy has designated FAMs to reduce IT applications to the minimum number needed to support Navy and Marine Corps requirements. This reduction process standardizes versions to a single application and selects certain applications or suites of applications to perform specific functions across the NMCI Enterprise. It eliminates applications that are not compliant with NMCI standards.

FAMs are responsible for enterprise management of applications and databases assigned within their functional areas (FAs).

**NOTE: *Only applications that have been allowed with restrictions and approved by the FAMs may be deployed in NMCI.***

The DON CIO has expanded the functionality of the current Department of the Navy Application Database Management System (DADMS) to support the FAM application rationalization process. Each Command has representatives working closely with the FAM on their applications and databases. Developers and program managers who have questions about the FAM processes should contact their Command FA representative or the FAM Lead.

Key to successful implementation of the FAM process is the participation of the Commands across the functional enterprise.

The operational taxonomy must be accurate to allow informed decisions by the FAMs on portfolio management of applications and systems that support specific operational activity requirements. FAMs are the final approval authorities for operational taxonomies and may modify operational taxonomies for their own FAs only. As stakeholders, FAMs may make change recommendations to other FAMs for consideration and approval.

FAMs are responsible for overall enterprise software management and the execution of specific responsibilities that include, but are not limited to the following:

- Oversee the activities of Functional Data Managers (FDMs).
- Meet process requirements for information gathering and consensus.
- Ensure that the FA has written mission statements, objectives, and a vision in place as a basis for analysis.
- Ensure that the FA has written internal policies in place to guide the FAM Partnership Team on internal FA issues and decisions.
- Cooperate in the identification and funding of required resources to support process execution.
- Cooperate in the identification of initiatives to help ensure that FA enterprise application-and-database management is achieved within the FA and across the enterprise.
- Monitor and approve the progress of the FAM Partnership Team through the major steps in the FAM Mid-Term Application and Database Rationalization Process, as appropriate.
- Control and assign authorities and privileges to Commands that are required to complete and maintain relevant sections of the Integrated Solution Framework (ISF) Tools Database/DADMS data-gathering tool.
- Maintain a relevant and accurate operational taxonomy in ISF Tools Database/DADMS.
- Identify and appoint the Functional Lead and Technical Lead for process execution.

#### **2.1.4.1 FAM Lead**

The FAM Lead develops and implements the process execution planning timeline with FAM approval.

#### **2.1.4.2 Functional Lead**

The Functional Lead performs the following tasks:

- Communicate formal intent and/or commitment to fully support FAM Mid-Term Application and Database Rationalization Process.
- Provide management oversight for process scheduling, resources, execution, and integration.
- Identify and appoint a FAM Partnership Team, with FAM approval.

#### **2.1.4.3 Technical Lead**

The Technical Lead may be a contractor or an in-service Government individual. At the discretion of the FAM, a contractor may be procured to form the basic FAM Partnership Team and to execute the entire process with assistance from designated FA SMEs. FA SMEs may be tasked to support contractor efforts on a full-time or part time basis.

#### **2.1.4.4 FAM Partnership Team**

The FAM Partnership Team provides the necessary expertise to execute the full spectrum of FA business and operational requirements analysis and validation for the FAs.

#### **2.1.5 Functional Data Manager (FDM)**

The FDM is responsible for implementing functional processes to produce and monitor the use of databases within and across FAs, information systems, and computing and communications infrastructures. FDMs are appointed by the FAMs and are responsible for the following tasks:

- Assist program managers and other system developers in registering system/application (metadata) and data exchange formats and maintaining the metadata baseline.
- Develop and maintain FA views of the DON data architecture.
- Develop candidate DoD standard data elements in coordination with the respective Functional Data Administrator (FDA).
- Coordinate with applicable stakeholders to ensure that DoD-proposed data standards are usable by DON systems.
- Designate the Authoritative Data Source (ADS) for its respective FAs and maintain the designation in the DADMS using processes and procedures approved by the DON CIO.
- Control and assign authorities and privileges required for completing and maintaining the applicable database information in DADMS, under their applicable FAM authority.

### **2.2 DESIGNATED APPROVAL AUTHORITY (DAA)**

#### **2.2.1 Navy NMCI DAA**

As the Navy NMCI DAA, NNWC has the responsibility and authority to decide whether to accept the security safeguards prescribed for an Automated Information System (AIS). The DAA is the official

authority responsible for issuing an accreditation statement that records the decision to accept those safeguards. The Navy NMCI DAA is responsible for the following tasks:

- Establish and promulgate the guidelines and security requirements applicable to the NMCI network and the software that operates on that network.
- Ensure the system accreditation for the enterprise.
- Ensure that the AIS security mechanisms enforce the security policy of the enterprise.
- Identify all security-related information required to support the FAM application and database management process.
- Ensure that security and information assurance data entered in the ISF Tools Database/DADMS is correct for each application and database.
- Remove all applications and databases from designated networks that are not included in the FAM portfolio of applications and databases in the ISF Tools Database/DADMS.
- Control and assign roles and responsibilities to designated personnel for completing and maintaining the security and information assurance data in the ISF Tools Database/DADMS.

## **2.2.2 Marine Corps NMCI DAA**

The Marine Corps CIO/Director C4 is the DAA for the Marine Corps. The DAA responsibility has been delegated to the IA branch head. Marine Corps NMCI DAA tasks include the following:

- Evaluate and approve/disapprove the connection of any application to the MCEN.
- Evaluate and approve/disapprove the connection of any application to the Marine Corps NMCI COI.

## **2.3 COMMANDER NAVAL NETWORK WARFARE COMMAND (NNWC)**

NNWC is the Navy central operational authority for space services, network, command and control, IT requirements, and information operations in support of Naval forces afloat and ashore. NNWC is responsible for the following tasks:

- Provide a single source of information support to the Fleet through assumption of central responsibility and authority over all aspects of IM.
- Serve as the advocate for operational forces in the development and fielding of IT, information operations, and space.
- Perform such other functions and tasks, as directed by higher authority.
- Provide approval authority for the deployment of all Navy releases into the NMCI environment.
- Prioritize and schedule releases for submission to EDS.
- Operate a secure and interoperable Naval network that enables effects-based operations and innovation.

- Coordinate and assess the Navy network, command and control, IT, information operations, and space requirements.
- Operate and maintain the Navy global IT systems and services, including enterprise networks, through assigned worldwide communications activities and related contracts that support Warfighting operations and command and control of Naval forces.
- Serve as the single focal point for Navy base-level communications policy, procedures, and resources, and operation and management of the Navy Base Level Information Infrastructure (BLII).
- Operate "Information Technology for the 21st Century" (IT-21) program to upgrade shipboard networks.
- Oversee the Navy computer network attack and defense work through IT-21 and the NMCI procurement with EDS.

### **2.3.1 NMCI Release Prioritization Manager (NRPM)**

The NRPM is an agent of NNWC responsible for the management of the Request to Deploy (RTD) process and establishing a priority for all releases submitted for deployment in NMCI. See [Section 6.0](#) for more details on the NRDP process.

### **2.3.2 NMCI Release Scheduling Manager (NRSM)**

The NRSM is an agent of NNWC responsible for assigning all releases a scheduled date for submission to the Applications Lab for processing. See [Section 6.0](#) for more details on the NRDP process.

## **2.4 MARINE CORPS NETWORK OPERATIONS SECURITY COMMAND (MCNOSC)**

The MCNOSC provides global network operations and computer network defense of the MCEN in order to facilitate seamless information exchange in support of Marine and Joint Forces operating worldwide. The MCNOSC concurrently provides technical leadership for service-wide initiatives that utilize the enterprise capabilities delivered by the MCEN.

The MCNOSC exploits networking expertise and technologies to expand and enhance services to the war fighter so that the network is developed as a weapon to achieve decision superiority. The MCNOSC is responsible for the following:

- Control day-to-day NMCI network operations and C2 Operation Cell (CCOC) within the Marine Corps COI.
- Direct operational execution and contractor interface.
- Coordinate enterprise network operations with Director NMCI and Commander NNWC.
- Provide Tactical & Deployed Support /Computer Network Defense (CND).
- Implement policy formulated by HQMC C4.
- Act as primary interface with the NMCI contractor for network operational, performance, and technical issues.
- Coordinate with and take direction from US STRATCOM chain of command for the defense of the NMCI.

- Act as primary Marine Corps interface with the DISA Global Operations Support Center (GOSC).
- Monitor and collect real-time data and provide to PM NMCI in support of their contractor performance evaluation efforts.

## **2.5 NAVY NMCI PROGRAM MANAGEMENT OFFICE (PMO)**

### **2.5.1 Enterprise Application Group for Legacy and Emerging (EAGLE)**

The Navy PMO created the EAGLE Team to focus on the following information:

- Critical Joint Applications (CJAs) listed in the NMCI contract
- Developer- or Command-owned applications in order to certify applications once at the enterprise or developer's level rather than retesting and certifying applications at each individual site
- All application related information in order to provide the focal point for the Site Solutions Engineering (SSE) teams.

The EAGLE Team is divided into the following teams:

- Data Management Team (DMT)
- NMCI Software Configuration Management (NSCM)
- Claimant CDA Support (CCS)
- Quarantine Upgrade Emerging Support Team (QUEST)
- NSCM Application Prioritization and Scheduling Team
- QUEST Regional Deployment Team (Q-RDT)

#### **2.5.1.1 Data Management Team (DMT)**

The DMT performs the following tasks:

- Maintain the ISF Tools Database as the “data repository” for all applications deployed in NMCI.
- Oversee accuracy and data integrity and maintain consolidated application data in one central and accessible location.
- Provide tool configuration, data cleanup, and maintenance.
- Support all levels of users throughout all steps of the transition process and the developer submission process.
- Reduce the amount of rework required by the developer and by each site team on previously encountered applications.

#### **2.5.1.2 NMCI Software Configuration Management (NSCM)**

The NSCM organization supports the NMCI PMO by providing management oversight and tracking of releases submitted for deployment in NMCI. The NSCM organization coordinates its efforts with the EDS Application Program Managers (APMs) to facilitate the test, certification, and deployment of

application releases to the NMCI enterprise. The NSCM acts as a liaison between a myriad of NMCI activities and helps to resolve issues.

The NSCM is responsible for the following tasks:

- Process, prioritize, and schedule RTD-sponsored applications.
- Technically review Release Deployment Plans (RDPs) and document the Test, Certification, and Deployment processes.
- Provide metrics reporting and application status to developers, NNWC, EDS, and the NMCI PMO.
- Provide training and education to developers through quarterly NMCI conferences.
- Develop and maintain internal processes for processing, tracking, and reporting status throughout the test and deployment life-cycle.
- Provide direct supervision and management of NSCM internal QUEST and CCS activities.
- Track status of Navy NMCI Interim Authority to Operate (IATO)/Authority to Operate (ATO) through the NNWC DAA approval process for RTD applications.
- Develop, maintain, and disseminate messages on the communication test, certification, and deployment status during the various stages of the RTD process.
- Identify RTD-developed NMCI enterprise solutions for quarantine/kiosk applications to reduce the legacy network and to eliminate dual desktops.

### **2.5.1.3 Claimant CDA Support (CCS)**

The CCS focuses on educating developers on the requirements for the Development, Testing, Certification, and Deployment processes in NMCI enterprise. The CCS performs the following specific tasks:

- Provide guidance in the collection and submission of media.
- Create Central Design Activity Request for Service (CDA RFS) documentation.
- Act as technical liaison with EDS throughout the process.
- Use ISF Tools Database to store and collect application information.
- Engage developers for legacy and enterprise application solutions.
- Provide metrics and reporting status to NMCI PMO, NNWC, and developers.
- Assist developers with the ISF Tools Database.

### **2.5.1.4 Quarantine Upgrade Emerging Support Team (QUEST)**

The QUEST organization was created to facilitate and support an integrated approach to quarantine/kiosk application solutions, upgraded applications, and new (emerging) applications to transitioned organizations within the NMCI Enterprise. QUEST supports the deployment of upgraded and new (emerging) applications as they move through the RTD process. QUEST works closely with the NSCM CCS to ensure that the required deployment/implementation documentation is submitted on time and in sufficient detail to support deployment. QUEST provides training and coordination to NMCI Activities,

e.g., Legacy Application Point of Contact/ Contract Technical Representative (LAPOC/CTR), EDS, NMCI PMO personnel, etc.

The QUEST organization consists of the following personnel:

- QUEST Coordinator
- QUEST Deployment Analyst
- ECCB/Network Operations Center (NOC)/Test Coordinators
- NNWC – EDS Liaisons
- Application Coordinators
- Field Representatives
- Communications Coordinator

### **QUEST Coordinator**

The QUEST Coordinator can be contacted at [NMCI\\_SCM@spawar.navy.mil](mailto:NMCI_SCM@spawar.navy.mil) and performs the following tasks:

- Coordinate all assets to support the deployment of applications to NMCI users.
- Conduct weekly teleconferences with the QUEST field representatives and the EDS APM lead regarding application deployment issues.
- Provide guidance and instruction to QUEST Network Operations Center (NOC), Service Request Management (Move/Add/Change - MAC), quarantined applications (QAPS), ECCB, unplanned, planned, and critical applications coordinators.

### **QUEST Deployment Analyst**

The QUEST Deployment Analyst performs the following tasks:

- Receive, audit, and perform technical review of required deployment documentation, ensuring an appropriate level of detail for deployment of a RTD application.
- Coordinate with appropriate activities to clarify and correct discrepancies.
- Forward the finalized RDP upon completion of the review to APM to support ECCB and NOC deployment activities.

### **ECCB/NOC/Test Coordinators**

The ECCB/NOC/Test Coordinators perform the following tasks:

- Resolve deployment issues and concerns.
- Request deployment reports.
- Establish close relationships with key personnel.

### **NNWC – EDS Liaisons**

The NNWC – EDS Liaisons perform the following tasks:



- Monitor application progression through the process..
- Update the Plan of Action and Milestones (POA&M). .
- Track media submission to the Applications Lab in San Diego, CA.
- Provide application reporting to NNWC, NMCI-PMO, and the NSCM Team.

## **Application Coordinators**

Application Coordinators perform the following tasks:

- Monitor the status of all NNWC-approved unplanned RTD applications, planned, quarantine/kiosk , and critical applications that are submitted for testing, certification, and deployment under the RTD process.
- Interface with scheduling, testing, and deployment activities to identify issues and to provide solutions.

## **Field Representatives**

Field Representatives perform the following tasks:

- Facilitate an integrated approach to upgrade and new (emerging) applications deployment and dual desktop resolution to transitioned organizations within the NMCI enterprise.
- Act as the liaison from the local sites to the NRDDG process.
- Work closely with Contract Technical Representatives (CTRs), Activity Contract Technical Representatives (ACTRs), LAPOCs, CIOs, and Commands to provide information, education, and deployment recommendations in the NMCI post transition environment.

## **Communications Coordinator**

The Communications Coordinator performs the following tasks:

- Send informational email messages to facilitate the transition of quarantine/kiosk and new (emerging) applications.
- Communicate the various stages of the RDP to the developer.

### **2.5.1.5 QUEST Release and Deployment Analyst (Q-RDA)**

The Q-RDA section is collocated within the NSCM facility. QUEST support can be requested through email at [NMCI\\_SCM@spawar.navy.mil](mailto:NMCI_SCM@spawar.navy.mil). The Q-RDA performs the following tasks:

- Provide training and education to LAPOC and CTR/ACTR personnel on the quarantine/kiosk mitigation, application upgrade, and new (emerging) application RDP.
- Work closely with the EDS APMs to ensure that the RDP information is relevant to the Deployment process.
- Engage the EDS APM and Service Request Support (SRS) personnel to coordinate critical information requirements during all phases of the application Deployment process.

- Notify the Q-RDT of impending application upgrade/new (emerging) releases and supporting RDPs.
- Facilitate quarantine/kiosk solutions across multiple regions.
- Provide deployment status and data reporting to NNWC and the NMCI PMO.
- Coordinate application quarantine/kiosk migration, application upgrade, and new (emerging) application activities with the following groups:
  - LAPOC, CTR/ACTR (site)
  - EDS Base Operations (Base Ops)
  - NMCI NOC
  - EDS Service Request Management (SRM) (MAC) Desk
  - Information Assurance Tiger Team (IATT) (quarantine/kiosk reduction)
  - EDS APMs
  - NNWC
  - EAGLE Claimant CDA Support (CCS) personnel.

#### **2.5.1.6 NSCM Application Prioritization and Scheduling Team**

This team prioritizes and schedules RTD application releases for testing based on priority, requested deployment date, media availability, deployment status, and the availability of test and certification resources.

#### **2.5.1.7 QUEST Regional Deployment Team (Q-RDT)**

The five Q-RDT field activities are located in the Southwest, Northwest, Hawaii, Southeast, and Northeast NMCI regions. The Q-RDT performs the following tasks:

- Provide onsite support to NMCI site personnel.
- Provide appropriate NMCI PMO regional oversight for the NMCI Application Deployment and Migration process.
- Coordinate with LAPOC, CTR/ACTR, EDS Base Ops, and NMCI Help Desk personnel to support required Test/Pilot Deployment and Notification Plans.
- Train site personnel on the RDP.
- Review existing quarantine plans and application to seat documentation in support of deployment planning.
- Coordinate application quarantine migration, application upgrade, and emerging (new) application activities with the following groups:
  - LAPOC, CTR/ACTR (site)
  - EDS Base Ops
  - IATT (quarantine reduction)
  - EDS APMs

- NNWC
- EAGLE CCS Activity

## **2.6 MARINE CORPS NMCI PMO**

### **2.6.1 Marine Corps Systems Command – Information Systems and Infrastructure (MCSC ISI)**

The MCSC ISI provides strategic leadership to ensure the timely delivery and sustainment of interoperable, integrated, and quality information technology (systems and infrastructure) and to position the Product Group (PG) to meet the future needs of the Marine Corps.

### **2.6.2 Program Manager NMCI Inspection/Test Instruction (ITI)**

#### **2.6.2.1 Program Manager NMCI ITI**

The Program Manager NMCI ITI performs the following tasks:

- Serve as the single authoritative source for all Marine Corps NMCI-related information.
- Provide communications guidance and program-level feedback.
- Provide information updates through Monthly NMCI Naval message SITREPS as appropriate.

#### **2.6.2.2 PM NMCI/ITI Staff**

The Program PM NMCI/ITI staff performs the following tasks:

- Serve as NMCI SMEs and web site content managers in all areas of program management and execution.
- Participate in NMCI Working Groups/integrated product teams (IPTs), as appropriate within their FAs of expertise.

### **2.6.3 Program Manager Enterprise Business Systems Support (EBSS)**

The PM EBSS provides effective software lifecycle management for Marine Corps enterprise business information systems in a timely, accurate, and cost-efficient manner, enabling functional area managers to support the Marine Warfighter's mission. EBSS supports the Marine Corps NMCI PMO by providing management oversight, tracking, and Precertification of application releases and facilitates the deployment of applications into the NMCI environment.

To facilitate start-to-finish NMCI application certification and deployment for the Marine Corps, EBSS performs the following tasks:

- Serve as the single POC to support deployment of applications for the Marine Corps into the NMCI environment.
- Advise and assist Marine Corps FAMs/application sponsors and developers throughout the NRDP.
- Ensure Marine Corps process integration with the NRRDG.

- Coordinate application release efforts with the Marine Corps Application Sponsors and EDS Application Project Managers (APMs) to track and monitor the status of application releases, provide liaison between the Marine Corps Application Sponsor and APM, assist in the resolution of problem areas, and coordinate deployment activities.
- Serve as liaison for Director, NMCI, EDS Applications Test Lab, HQMC C4, MCNOSC, PM NMCI and Joint PMs.
- Manage and maintain Marine Corps Applications and Integration Testing (MCAIT) Lab to support existing and new (emerging) applications.
- Provide Precertification of applications for NMCI Functional and IA Compliance.
- Provide Advance Publisher .msi packages for submission to EDS Applications Test Lab.
- Assist in ARDRA/Pilot Test and deployment process.
- Serve as the Marine Corps NMCI Release Scheduling Manager.
- Schedule applications for pre-certification at the MCAIT Lab in accordance with prioritization set by HQMC (C4), and coordinate prioritization and scheduling for final certification and deployment at EDS Applications Test Lab.
- Integrate and maintain MCASE database for tracking Requests to
- Deploy (RTD)
- Interface MCASE information with ISF Tools Database and DADMS.
- Serve as the Marine Corps NMCI Software Configuration Manager.
- Ensure enterprise level configuration management of applications and minimize scheduling delays in deployment through the implementation of change and configuration management policies, procedures, and processes in compliance with NRDDG.
- Serve as the web site content manager for USMC NMCI application processes.

## **2.7 COMMAND RESPONSIBILITIES**

This section addresses roles and responsibilities of a Command. A Command is defined as a Navy claimant or Echelon II or Marine Corps Forces Command (i.e., MARFORPAC, MARFORLANT, and MARFORRES).

### **2.7.1 Sponsoring Command**

- Report to CNO or higher as a normal part of operations.
- Exercise application management over all subordinate units or organizations.
- Is supported by the Program of Record-Program Manager (POR-PM) and developer.
- Provide program and content oversight of the applications and releases.
- Play a review and approval role in the RTD.

## **2.7.2 Program of Record Program Manager ((POR-PM)**

The Program of Record (POR) is a formally funded program or system in support of Navy and Marine Corps requirements. The Program Manager (PM) for a POR is an office or individual who has program responsibilities for an application. These responsibilities include, but are not limited to, funding and maintaining the application. The POR-PM tasks include the following:

- Conduct periodic reviews of their applications to determine if they are current or require a more detailed review and update.
- In conjunction with the developers and FAMs, develop a strategy to retire obsolete applications.
- Conduct periodic reviews to ensure that only current applications are in service.

## **2.7.3 Developer**

A developer is a vendor, organization, or segment of an organization within a DoD component that develops, modifies, maintains, tests, documents, and deploys significant IT/National Security System (NSS) software and its associated support functions and activities substantially in-house. Excluded are organizations that primarily serve in the inherently Governmental role related to the acquisition and management oversight of software systems, e.g., Program Executive Offices (PEOs), PMs, and Special Project Offices (SPOs).

Significant IT/NSS software is defined as software that meets one or more of the following criteria:

- In use Major Command-wide, Component-wide, at multiple installations, or in a broader scope.
- Support DoD/Component business processes.
- Constitute mission critical/essential system(s).
- Consist of multiple nonmission critical/essential applications.

Associated support functions and activities relate to software development such as requirements, design, code, test, documentation, CM, replication/distribution, training, operations, development environment support, field support, and user assistance.

For the purposes of this guide, a developer is any organization, site, group, department, division, unit, section, or individual or Government-sponsored contractor or vendor, who wants to introduce a new (emerging) application or change to an existing application within NMCI environment.

Developers are responsible for ensuring that their releases are compliant with Navy information assurance, boundary, and GPO policies prior to deployment within NMCI. Developers are responsible for adhering to the requirements for developing and migrating applications that comply with TFW, NMCI, IT-21, Outside-Continental United States (OCONUS) BLII architectures, and DON standards.

## **2.8 ELECTRONIC DATA SYSTEMS (EDS)**

EDS provides strategy, implementation, business transformation, and operational solutions for digital enterprises. EDS is the prime contractor supporting NMCI.

### 2.8.1 Applications Lab

Developers are responsible for providing an Application Submission Packet to the Applications Lab in accordance with Section 6.0. The Applications Lab has both an unclassified application testing facility and a separate classified application testing facility.

Upon receipt of the Application Submission Packet, the Applications Lab is responsible for completing the processes contained in Section 6.0 that support the introduction of new (emerging) applications and updates, upgrades, patches, fixes, and quarantine/kiosk solutions for existing applications.

### 2.8.2 Site Manager (SM)

The SM, also referred to as Base Operations Manager (BOM), is the lead representative of EDS at each site. The SM is responsible for the delivery of all NMCI services at the designated location. The SM has the following service-delivery roles:

- Support "as-is" applications during the Assumption of Responsibility (AOR) od.

**NOTE:** AOR is the date when responsibility for operating the “as-is” environment and for work defined by the ordered NMCI CLINs shifts from the Government and its local contractors to the ISF.

- Support migration/transition during the cutover period.
- Support post transition daily production of existing and new Navy requirements.
- Coordinate EDS operations for the site.

### 2.8.3 Enterprise Change Control Board (ECCB)

The ECCB is composed of IA and operations personnel from EDS, the Navy, the Marine Corps, and the PMO. Section 6.0 provides more detailed explanation of the ECCB process. Tasks include the following:

- Assess the overall risk exposure.
- Examine whether the application is needed in the enterprise.
- Review all submitted documentation.
- Approve releases that meet all ECCB requirements to continue in the deployment process. .

### 2.8.4 Application Project Manager (APM)

An EDS APM is assigned to each new (emerging) application or application change that enters the Deployment process. The APM is responsible for moving the application through the process and coordinating all tasks and teams required to meet this goal. The APM performs the following tasks:

- Notify the Navy PMO and developer of the assignment to manage the application deployment project.
- Act as the single POC for all status information of an application in the Deployment process for the PMO and the developer.
- Manage the application throughout the Deployment process and coordinate the required work by different EDS teams to accomplish the NMCI Certification and Deployment.

- Update application project information in Project InVision (PIV) to correct the weekly dashboard status.
- Create and submit the Request for Change (RFC) form and collect materials for the submission package for ECCB.
- Coordinate the ECCB presentation and invite the developer and PMO representatives to support the presentation (as needed).

### **3.0 NMCI RELEASE MANAGEMENT PROCESS (NRMP)**

This section covers the NRMP that is jointly managed by the Navy and Marine Corps FAMs, NNWC, HQMC C4, ISI/EBSS Commands, and developers. Its primary focus is NMCI and the aspects of release management that directly affect sustainment of existing applications, deployment of new (emerging) applications, and installation of existing applications in the post transition environment. To achieve this goal, this section includes the following areas:

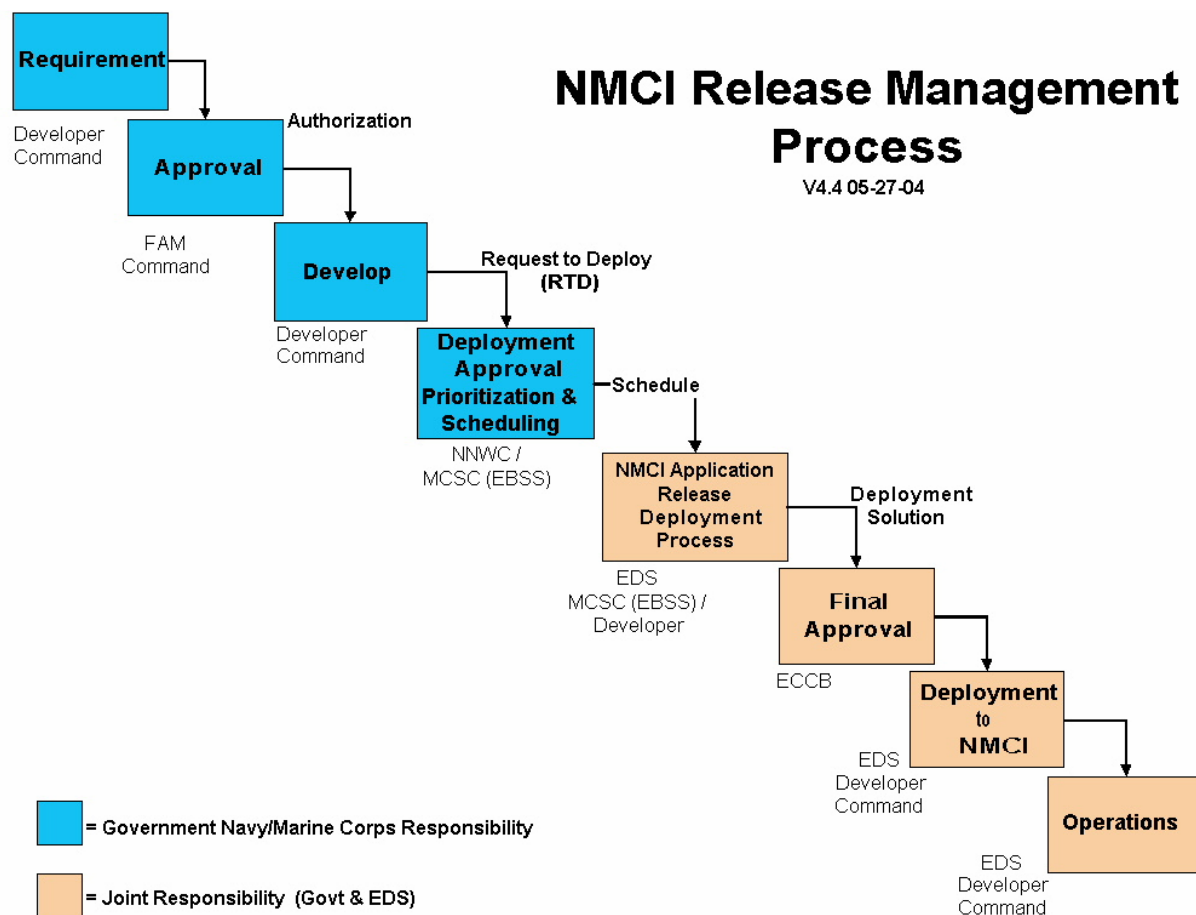
- NMCI Release Management Process (NRMP) – The four logical areas that provide a standardized software management system:
  - Approval
  - Development
  - Deployment
  - Sustained Operations
- Software Definitions and Processing Requirements
- Requesting Release in the Post Transition Environment (RRPTE)

The developers and Commands also need a clear understanding of the policy, procedures, guidelines, and processes in order to sustain applications contained in their rationalized application list and deployed in NMCI in the post transition environment.

Section 6.0 provides the policy, procedures, guidelines, and processes that support the NMCI Request Deployment Process (NRDP), including the RTD.

Figure 3-1 displays the steps in the NRMP that developers and Commands must follow to obtain development approval from the FAM and deployment approval from NNWC and HQMC C4.





**Figure 3-1 NMCI Release Management Process**

## 3.1 APPROVAL

### 3.1.1 Requirement Determination

The Government is responsible for determining whether to sustain an existing application or to introduce a new (emerging) application to support an operational or business requirement. Introduction of new (emerging) applications may include the deployment a GOTS or COTS application. A developer or Command may also deploy an application that is currently certified and deployed within NMCI to a new site.

### 3.1.2 FAM Approval

The FAM is the designated approval granting authority for the development of applications and releases that operate within NMCI. The developer must be granted approval prior to beginning work on the development or acquisition of an application or release. This includes the introduction of a new (emerging) application that has not previously been developed. Developers must use DADMS and complete the FAM Application Rationalization Questionnaire in order to be granted approval by the FAM. [Appendix H](#) lists the current FAMs for both the Navy and Marine Corps.

## **3.2 DEVELOPMENT**

FAM approval authorizes the developer to proceed with the development or acquisition of the desired application or release. The NRDDG provides the developer with background information pertaining to NMCI-specific compliance standards. Refer to Section 5.0 for details on the Development process.

## **3.3 DEPLOYMENT**

The NRDP is a multifaceted process that entails a significant effort to ensure that all releases are properly packaged, tested, and certified prior to deployment in NMCI. Section 6.0 provides detailed information on the NRDP. In order to support the sustainment of existing applications and the introduction of new (emerging) releases, a disciplined approach has been established to manage the processing of these releases. The initial requirement is to clearly define the various types of releases, the nature of the changes being implemented, and the number of opportunities for submitting releases into the NRDP.

## **3.4 SUSTAINED OPERATIONS**

This is the phase in which required applications have been tested, certified, and deployed in NMCI and have achieved a steady state of operation. Sustained operations are beyond the scope of this guide.

## **3.5 SOFTWARE DEFINITIONS AND PROCESSING REQUIREMENTS**

The following paragraphs define the different types of applications that operate on or interact with desktops in the NMCI environment. In some cases, the applications are not deployed on the desktop and are accessed through the use of a common front-end browser or terminal emulation. The NMCI Gold Disk loadset includes both Internet browser and terminal emulation software as part of the standard desktop configuration.

### **3.5.1 Client/Desktop/Standalone (Simple) Applications**

These nonnetworked applications perform their functionality on the local desktop. They do not include dependencies or requirements to print through network services or to save to corporate/shared drives. A simple test to verify if an application is considered client only is to disconnect the desktop from the network. If the application functions successfully, it is most likely a standalone (simple) application.

### **3.5.2 Web Applications**

These applications exist onboard a web server within the NMCI enclave, including the demilitarized zone (DMZ), or operate outside NMCI. They have the following characteristics:

- Use a common front-end browser (i.e., Netscape Navigator or Internet Explorer) on the desktop to provide client connectivity and functionality.
- Use hypertext transfer protocol (http) (port 80) or hypertext transfer protocol secure (https) (secure socket layer - SSL port 443) per the World Wide Web Consortium (W<sup>3</sup>C) standards.

### **3.5.2.1 Simple Web Applications**

These applications have no external dependencies outside the Gold Disk components and the web server interface. The entire functionality of these applications, except for the presentation through the browser, executes on the web server. They have the following characteristics:

- Do not require other client executables outside the common front-end browser and related Gold Disk components (i.e., plug-ins, mobile code, etc.).
- Do not attempt to download or install any executable (.exe) from the server to the client during the operation of the application.

### **3.5.2.2 Complex Web Applications**

These applications depend on external executables on the desktop, as well as execution on the web server. NMCI handles complex web applications in the same manner as client/server applications. A complex web application has the following characteristics:

- Require other client executables outside the common front-end browser and related Gold Disk components to connect to the host web site.
- Attempt to download or install executables (.exe) to the client during the operation of the application. These include plug-ins, mobile code, compiled binary executables, etc.

### **3.5.3 Server-Based Applications**

These applications exist on a server within the NMCI enclave, including the DMZ, or operate outside NMCI. They are not web-based applications and have the following characteristics:

- Perform all operations on the server, except for their input/output and presentation interface performed by a terminal emulator (such as Reflection, CITRIX ICA, etc.).
- Do not have an associated client executable, but rely on server console input/output.

### **3.5.4 Client/Server Application**

These networked applications have a client front end on an NMCI seat and interface with the back end of the application on an NMCI or legacy server. Client/server applications have an executable that runs on the a user's desktop and a server executable that may interface with databases or other executables. They include complex web applications that download or install executable(s) (.exe) to the client during the execution of the application.

### **3.5.5 Application Decision Logic Table (DLT)**

Table 3-1 provides scenarios to help clarify when an application must be submitted to EDS for processing and deployment, when it is reviewed by the ECCB, and the type of Certification and Accreditation (C&A) tasks required to support the release.

**Table 3-1 NMCI Application DLT**

<b>NMCI Application DLT</b>					
<b>Rule</b>	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>
	<b>When the release is a</b>	<b>and</b>	<b>then the release</b>	<b>and</b>	<b>and the release</b>
1	Client/Desktop/ Standalone application being introduced or upgraded	Operates or will operate on an NMCI seat	Must undergo NMCI Release Deployment processing in accordance with the NRDDG. (Note 1)	Is reviewed by the ECCB (Note 2)	Will receive an ATO from the NMCI DAA upon certification. (Note 3)
2	Client/Desktop/ Standalone application being introduced or upgraded	Will not operate on an NMCI seat	Does not undergo NRDP in accordance with the NRDDG.	Is not reviewed by the ECCB (Note 4)	Requires C&A by the responsible Navy Command DAA. (Note 5)
3	New web application being introduced that - Does not require external plug-ins, mobile code , or executables on the desktop - Uses standard web ports, protocols, and services for access.	Web server resides inside NMCI (to include the DMZ)	Does not undergo NRDP in accordance with the NRDDG	Is reviewed by the ECCB	Requires DoD Information Technology Security Certification and Accreditation Process (DITSCAP) to verify ports, protocols, and services and must receive IATO/ATO from NMCI DAA as a new (emerging) application.
		Web server resides outside the NMCI environment		Is not reviewed by the ECCB (Note 6)	Does not require DITSCAP. (Note 7)
4	New web application being introduced	Web server resides inside NMCI (to include the DMZ)	Must undergo NRDP in accordance with the NRDDG to	Is reviewed by the ECCB (Note	Requires DITSCAP to verify ports, protocols, and

<b>NMCI Application DLT</b>					
<b>Rule</b>	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>
	<b>When the release is a</b>	<b>and</b>	<b>then the release</b>	<b>and</b>	<b>and the release</b>
	requires external plug-ins, mobile code, or executables on the desktop	Web server resides outside the NMCI environment	certify the external plug-ins, mobile code, or executables for the desktop. (Note 1)	8)	services and must receive IATO/ATO from NMCI DAA as a new (emerging) application. (Note 9)
5	Existing web application being upgraded that - Does not have nor require upgrades to external plug-ins, mobile code, or executables on the desktop - Uses standard web ports, protocols, and services for access - Is essentially, web-site content changes only	Web server resides inside NMCI (to include the DMZ)	Does not undergo NRDP in accordance with the NRDDG	Is not reviewed by the ECCB (Note 6)	Does not require an updated DITSCAP as long as ports, protocols, and services remain unchanged. Update to the existing DITSCAP is required by system owner.
		Web server resides outside the NMCI environment			
6	Existing web application being upgraded that requires changes in one or more of the following: - Plug-ins - Executables - Mobile code - Ports, protocols, and services	Web server resides inside NMCI (to include the DMZ)	Must undergo NRDP in accordance with the NRDDG. (Note 1)	Is reviewed by the ECCB (Note 8)	Requires an updated DITSCAP to reflect ports, protocols, and services changes. NMCI DAA issues new IATO/ ATO. (Note 9)
		Web server resides outside the NMCI environment			

<b>NMCI Application DLT</b>					
<b>Rule</b>	<b>A</b> <b>When the release is a</b>	<b>B</b> <b>and</b>	<b>C</b> <b>then the release</b>	<b>D</b> <b>and</b>	<b>E</b> <b>and the release</b>
7	New Client/Server application being introduced	Server resides inside NMCI (to include the DMZ) and the desktop resides in the NMCI environment	Must undergo NRDP in accordance with the NRDDG to certify the client end and connection to the server. (Note 1)	Is reviewed by the ECCB (Note 2 & 10)	Requires an DITSCAP to verify ports, protocols, and services and must receive IATO/ATO from NMCI DAA as a new (emerging) application pending submission of DITSCAP compliance . (Note 9)
		Server resides outside the NMCI environment and the desktop resides in the NMCI environment			
		Server resides outside the NMCI environment and the desktop resides in the NMCI environment			
8	Existing Client/Server application being upgraded that - Does not change the client end - Does not change network topology (ports, protocols, and services) - Is essentially, server content changes only	Server resides inside NMCI environment (to include the DMZ) and the desktop resides in the NMCI environment	Does not undergo NRDP	Is not reviewed by the ECCB	Does not require an updated DITSCAP as long as ports, protocols, and services remain unchanged. Update to the existing DITSCAP is required by system owner.
		Server resides outside the NMCI environment and the desktop resides in the NMCI environment			
9	Existing Client/Server application being upgraded with changes to one or both of	Server resides inside NMCI (to include the DMZ) and the desktop resides in the NMCI environment	Must undergo NRDP in accordance with the NRDDG to certify the client end and connection	Is reviewed by the ECCB (Note 2 & 10)	Requires an updated DITSCAP to verify ports, protocols, and services and is

<b>NMCI Application DLT</b>					
<b>Rule</b>	<b>A</b> <b>When the release is a</b>	<b>B</b> <b>and</b>	<b>C</b> <b>then the release</b>	<b>D</b> <b>and</b>	<b>E</b> <b>and the release</b>
	the following: - Client end - Network topology (ports, protocols, and services)		to the server. (Note 1)		issued new ATO/ IATO from NMCI DAA. (Note 9)
10	New server-based application being introduced	Server resides inside NMCI environment (to include the DMZ)	Must undergo NRDP in accordance with the NRDDG to verify ports, protocols, services, and connectivity. (Note 1)	Is reviewed by the ECCB (Note 10)	Requires DITSCAP to verify ports, protocols, and services and must receive IATO/ATO from NMCI DAA as a new (emerging) application. Pending submission of DITSCAP compliant DITSCAP. (Note 9)
		Server resides outside the NMCI environment			
11	Existing server-based application being upgraded with no changes to the following: - Network topology (ports, protocols, and services) - Hardware - Desktop software, including scripts - Operating system - Keyboard mapping	Server resides inside NMCI environment (to include the DMZ)	Does not undergo NRDP in accordance with the NRDDG	Is not reviewed by the ECCB	Does not require an updated DITSCAP as long as ports, protocols, and services remain unchanged. Update to the existing DITSCAP is required by the system owner.

<b>NMCI Application DLT</b>					
<b>Rule</b>	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>
	<b>When the release is a</b>	<b>and</b>	<b>then the release</b>	<b>and</b>	<b>and the release</b>
	- Is essentially, changes to server content only				
		Server resides outside NMCI environment			
12	Existing server-based application being upgraded with changes to one or more of the following: - Network topology (ports, protocols, services) - Hardware - Desktop software, including scripts - Operating system - Keyboard mapping	Server resides inside NMCI environment (to include the DMZ)  Server resides outside the NMCI environment	Must undergo NRDP in accordance with the NRDDG. (Note 1)	Is reviewed by the ECCB (Note 2 & 10)	Requires an updated DITSCAP to verify ports, protocols, and services and is issued new ATO/ IATO from NMCI DAA. (Note 9)

1. Requires RTD and Request for Service (RFS).
2. All software installed on NMCI seats must undergo Certification and Change Control Management prior to deployment.
3. All simple releases that successfully complete Packaging, Testing, and Certification are granted an ATO by the Navy NMCI DAA.
4. Application is not installed within NMCI.
5. C&A by DAA per COMNAVNETWARCOM msg 071455Z AUG 03 Subj: Navy Designated Approval Authority Assumption.
6. Web server is outside NMCI and does not require reviews.
7. All Navy Commands are required to follow DITSCAP procedures for C&A of their application.



8. Web application impacts the NMCI seat. Desktop attributes must undergo Certification and Change Control Management prior to deployment.
9. All complex releases that successfully complete Packaging, Testing, and Certification are granted an IATO by the Navy NMCI DAA.
10. All hardware/software changes that impact NMCI environment must undergo Change Control Management approval.

### 3.5.6 NMCI Application Business Rules

The business rules govern the various scenarios for application and release deployment in the NMCI post-transition environment. They must meet the requirements shown in Table 3-2 and Table 3-3.

**Table 3-2. NMCI Post Transition Application Business Rules DLT**

<b>NMCI Post Transition Application Business Rules DLT</b>					
<b>Rule</b>	<b>A</b> <b>When the release is</b>	<b>B</b> <b>Then the release</b>	<b>C</b> <b>and</b>	<b>D</b> <b>Then the release</b>	<b>E</b> <b>and</b>
1	A New (Emerging) Application and is FAM approved.	Must follow the NRDDG process and requires a Certification CLIN. (Notes 1 & 2)	A cost is incurred for distribution since this is a New/ Emerging application.	Requires a Service Request (MAC) or Distribution CLIN for distribution of the new release. (Note 3)	Use the RRPTE process for users who were not mapped with the original distribution.
2	An Upgrade/Update to Existing Applications and is FAM approved.	Must follow the NRDDG process and requires a Certification CLIN. (Notes 1 & 2)	No cost is incurred for distribution to users of previous version as long as EDS does not have to manually touch the seat. (Note 4)	Requires a Service Request (MAC) or Distribution CLIN for distribution to new users. (Notes 3 & 5)	Use the RRPTE process for users who were not mapped with the original distribution.
3	A Quarantine/ Kiosk Remediation Solution: Deployment of New Solution that is FAM approved	Must follow the NRDDG process and requires a Certification CLIN. (Notes 1 & 2)	No additional cost is incurred for distribution to eliminate Dual Desktops as long as EDS does not have to manually touch the seat. (Note 5)	Quarantine/Kiosk seats must be registered in the DDR to qualify for no-cost distribution	Use the RRPTE process for distribution to non-Quarantine/Kiosk users (Note 3)

Rule	A	B	C	D	E
	When the release is	Then the release	and	Then the release	and
4	A Quarantine/Kiosk Remediation Solution: Using an existing Radia solution that is FAM approved	Does not follow the NRDDG process and does not require a Certification CLIN. (Note 6)	A cost is incurred for distribution.	Requires a Service Request (MAC) or Distribution CLIN to deploy to NMCI seats. Quarantine/Kiosk seats must be registered in the DDR. (Note 3)	Use the RRPTE process for distribution to non-Quarantine/Kiosk users (Note 3)
5	A Driver Supporting an Authorized Peripheral Device Not on the NMCI Seat	Does not follow the NRDDG process and does not require a Certification CLIN. (Note 6)	A cost is incurred for distribution. (Note 7)	Requires a Service Request (MAC). Must be coordinated with the local Base Operations personnel for distribution of the new driver. (Note 8)	

1. Requires a Request to Deploy (RTD), CDA RFS, and Release Deployment Plan (RDP).
2. Follows the NMCI Release Deployment Process (NRDP)
3. Application Mapping is a responsibility of the Government.
4. Existing users of the application who are in Active Directory, existing users of the application who are not in Active Directory but were part of the original deployment either manually/locally loaded, and is verified through DCAP.
5. Required for new users that were not part of the original mapping.
6. Does not require a RTD, CDA RFS, or RDP, since the release has already been tested and certified or is not an application.
7. Cost is determined based on the level of effort to load the drivers.
8. If the driver does not load successfully, then the customer may request reengineering services from EDS using CLIN 29 or obtain another driver that will successfully load.

### 3.5.6.1 Rule 1 New (Emerging) Applications

A new (emerging) application must receive FAM approval and follow the NRDDG process. The application requires a RTD, CDA RFS, and Release Deployment Plan (RDP) and must follow the NRDP. It requires the submission of Certification and Distribution CLINs to cover all costs. Application Mapping must be completed no later than 30 days prior to the completion of Certification. The RRPTE process must be used for users who were not mapped with the original distribution.

### 3.5.6.2 Rule 2 Upgrade/Update to Existing Applications

Upgrades/Updates must receive FAM approval and follow the NRDDG process. They require a RTD, CDA RFS, and RDP and must follow the NRDP. They require the submission of a Certification CLIN and a Service Request (MAC) or Distribution CLIN to cover all costs. No cost is incurred for distribution to users of previous version as long as EDS does not have to manually touch the seat. Application

Mapping must be completed no later than 30 days prior to the completion of Certification. The RRPTE process must be used for users who were not mapped with the original distribution.

### 3.5.6.3 Rule 3 Quarantine/Kiosk Remediation Solution (Deployment of New Solution)

A Quarantine/Kiosk remediation solution must receive FAM approval and must follow the NRDDG process. A new solution requires a RTD, CDA RFS, and RDP and must follow the NRDP. It requires the submission of a Certification CLIN and a Service Request (MAC) or Distribution CLIN to cover all costs. No additional cost is incurred for distribution that eliminates Dual Desktops as long as EDS does not have to manually touch the seat and must be registered in the DDR to qualify for no-cost distribution. The RRPTE process must be used for distribution to non-quarantine/kiosk users.

### 3.5.6.4 Rule 4 Quarantine/Kiosk Remediation Solution (Using an Existing Radia Instance)

A Quarantine/Kiosk remediation solution must receive FAM approval. Since the application has been previously certified and is in a certified, ready-to-deploy state, developers do not follow the NRDDG process nor develop an RTD, RDP, or CDA RFS. Developers do not submit a Certification CLIN but do use the Service Request Management (MAC) or the Distribution CLIN for deployment of the application. All quarantine/kiosk desktops must be registered in the DDR.

### 3.5.6.5 Rule 5 Driver Supporting an Authorized Peripheral Device Not on the NMCI Seat

This request does not follow the NRDDG process nor require a Certification CLIN, RTD, CDA RFS, or RDP, since it is not an application. The customers must be able to provide the operating-system-compatible drive software. They must submit a Service Request (MAC) and coordinate installation with the local Base Operations personnel.

**Table 3-3. NMCI Site/Command Application Request Business Rules DLT**

<b>NMCI Site/Command Application Request Business Rules DLT</b>					
<b>Rule</b>	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>
	<b>When the release is</b>	<b>Then the release</b>	<b>and</b>	<b>Then the release</b>	<b>and</b>
1	FAM approved, certified, has a Radia instance, electronic-deployment ready (L_, O_, or U_), and needed on the NMCI seat	Is deployed to the seat using the RRPTE. process (Note 1)	A cost is incurred for distribution since this application has not been previously deployed on the requested NMCI seat.	Requires a Service Request (MAC) or Distribution CLIN to deploy. (Note 2)	Repeat the RRPTE process for any additional users.

<b>NMCI Site/Command Application Request Business Rules DLT</b>					
<b>Rule</b>	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>
	<b>When the release is</b>	<b>Then the release</b>	<b>and</b>	<b>Then the release</b>	<b>and</b>
2	FAM approved, certified, manual-deployment ready (X_ or Y_), and needed on the NMCI seat	Is deployed to the seat using the RRPTE. process Locally loaded versions (X_ and Y_) can only be deployed at the original site (Note 1)	A cost is incurred for distribution since this application has not been previously deployed on the requested NMCI seat.	Requires a Service Request (MAC) or Distribution CLIN to deploy. (Note 2)	Repeat the RRPTE process for any additional users.

1. Does not require an RTD, CDA RFS, or RDP since the release has already been tested and certified.
2. Application Mapping is a responsibility of the Government.

### 3.5.6.6 Requesting a Release in the Post-Transition Environment (RRPTE)

For RRPTE, the release must receive FAM approval, be certified, have a Radia instance (L\_, O\_, or U\_), and be deployment ready. Locally loaded versions (X\_ and Y\_) can only be deployed at the original site. The release does not require an RTD, CDA RFS, or RDP, since it has already been tested and certified. A cost is incurred for distribution since this application has not been previously deployed on the requested NMCI seat. It requires the use of a Service Request (MAC) or Distribution CLIN to deploy. Repeat the RRPTE process for any additional users. The same process is followed for electronic and manually deployed applications.

### 3.5.6.7 Incomplete Transition (Cutover)

Incomplete Transition (Cutover) Applications must be compliant with FAM policies. The application must have been on the original transition Implementation Group Rationalized List and Workbook. It must have been part of the original seat mapping during transition. A Help Desk Trouble Ticket is used to resolve the problem. This resolution incurs no cost if it resulted from an EDS oversight during the original transition. If the application does not meet the above criteria but was missed, the RRPTE process should be used to resolve the deployment.

### Transition/Post Transition Government Off-the-Shelf (GOTS) Application Introduction Rule

Any GOTS application or release being introduced into NMCI, for which a previously deployed version exists, is introduced per the NRDDG, NRMP, and NRDP.

### Transition/Post Transition GOTS Application Introduction Rule Impact

Application developers may not introduce enterprise upgrades and updates into NMCI for applications already deployed in NMCI through a transitioning site or the Legacy Application Transition process as depicted in the LATG.

To upgrade or update applications already in NMCI, a developer or application owner must follow the process described in the NRDDG.

### **Transition/Post Transition GOTS Application Introduction Rule Exception**

Enterprise solution process through the EDS Application Lab is the preferred solution for deployment. If this release delays a transitioning site, the following business rules apply:

- Process and use a Legacy Application Deployment Readiness Activity (LADRA)-prepared local solution of that GOT to prevent cutover delays.
- Use this solution locally only until the enterprise solution is distributed.

### **3.6 REQUESTING RELEASE IN THE POST TRANSITION ENVIRONMENT (RRPTE)**

Figure 3-2 depicts the current process for a site that has completed cutover or is operating in the post transition environment to obtain a release that has already been tested and certified and is ready for deployment in the NMCI environment. A streamlined version of this process will be available in the near future. The streamlined version will leverage existing technology incorporated in the NMCI Enterprise Tool (NET) to support the online ordering and processing of all documentation. The NRDDG will be revised with the new RRPTE process when the capability within NET is ready for deployment. Figure 3-3 is the legend for process flow diagrams used throughout this guide.

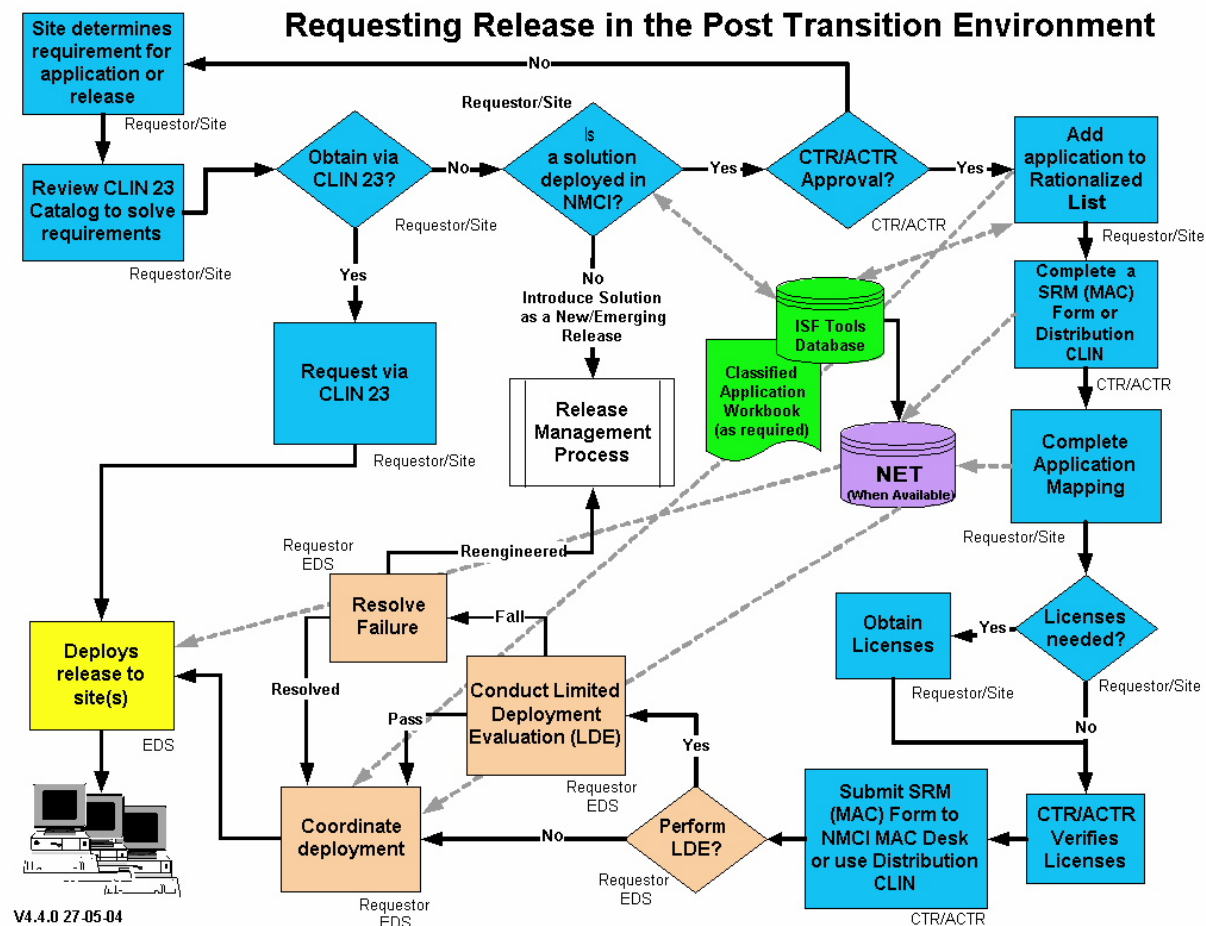
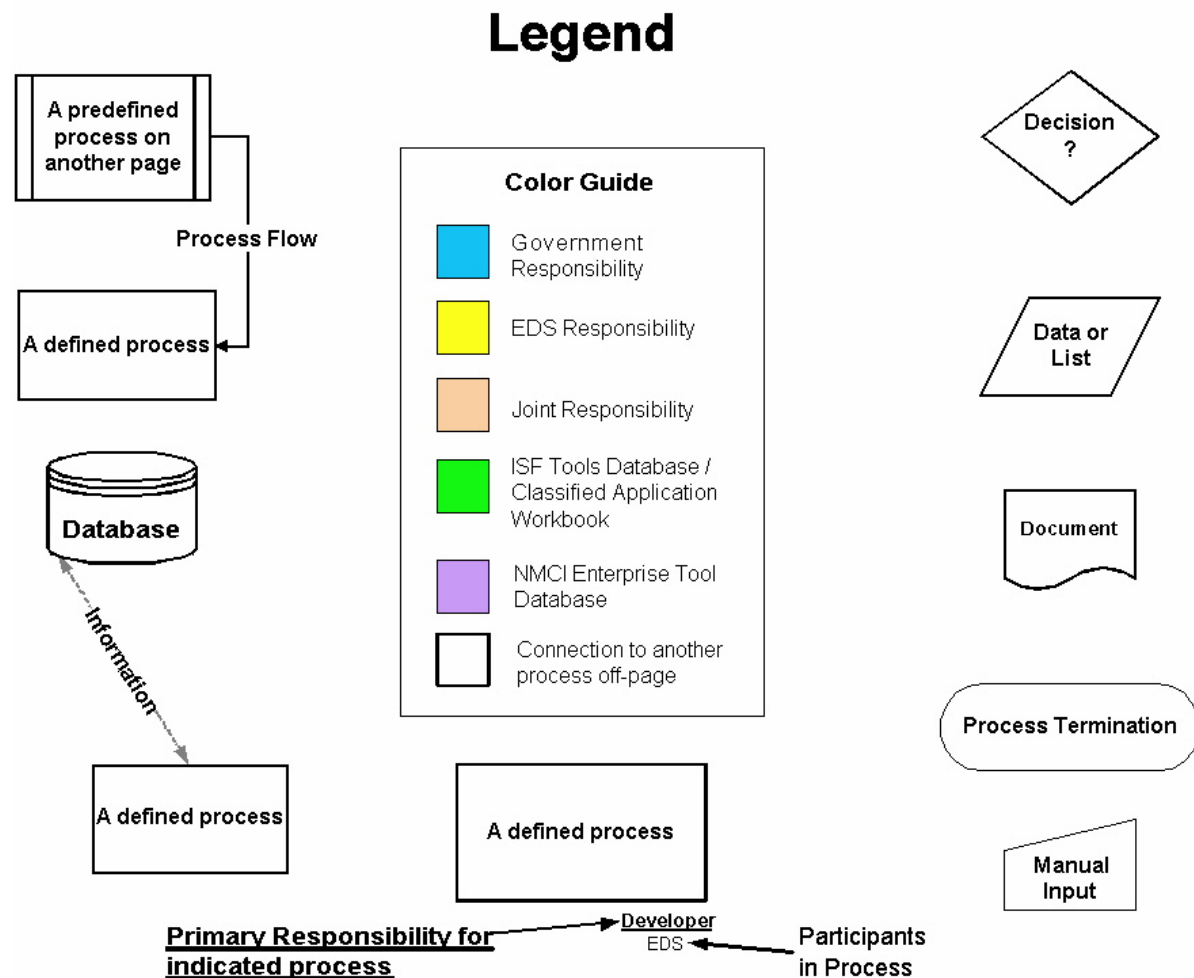


Figure 3-2 RRPTE



V4.4 05-27-04

**Figure 3-3 RRPTE Legend**

The following paragraphs cover the processing requirements to enable a Command/site to request and deploy a release that has already been packaged, tested, certified, and is ready to deploy within NMCI. Obtaining a release through this process is essentially characterized as an application “Pull”. Since only releases that have been previously packaged, tested, certified, and deployed (to include Ready for Deployment) can be obtained through this process, an RTD and RFS *will not* be required or submitted.

### 3.6.1 Requirement Determination

The requestor/site must first determine a requirement for an application that provides a solution for an existing or new business function. The site/Command employs its own decision-making process to determine the need for a particular application or release. This guide is not intended to tell a requestor or site how to determine this requirement.

### 3.6.2 Review Contract Line Item Number (CLIN) 0023 Catalog of Applications

The requestor/site must review the CLIN 0023 catalog to determine if a solution to support this requirement is available. Use of the CLIN 0023 solution is *optional*. If the site/Command can solve this

requirement by using one of the CLIN 0023 options, the process and steps to deploy the release are simplified for all parties involved. The site/Command can order the application item through its CTR/ACTR and deal directly with the ISF to deploy the release. The CLIN 0023 catalog can be found at <http://www.nmci-isf.com/>. If the solution is not available through the CLIN 0023 catalog, the requestor/user must proceed to the next step in the process.

### **3.6.3 Optional User Capabilities Catalog CLIN 0023**

This Optional User Capabilities Catalog provides commercial off the shelf (COTS) software and hardware peripherals associated with data, voice, and video seats, to support requirements beyond the basic services for specialized tasks. Items in the catalog can be ordered and provided to the requestor and are integrated and interoperate with all basic and optional services.

More detailed information is available at <http://www.nmci-isf.com/clin023.htm>

### **3.6.4 Solution Deployed in NMCI**

The requestor/site must review the NMCI Application Catalog located on the ISF Tools Database to determine if a solution has been packaged, tested, certified, and is either deployed or in a “Ready to Deploy” status. Note that requestor/site should use, if available, the certified Ready to Deploy CDA RFS version of the release. If a CDA RFS version is not available, the requestor/site should choose any available version that is marked certified Ready to Deploy. The requestor/site must specify the RFS number and Radia instance name wanted. Only those releases that have been approved by the FAM may be selected for deployment. If the application is not available in the NMCI Application Catalog, the requestor/site must introduce the solution as a new/emerging release by following the NRDP in Section 6.0.

### **3.6.5 Contract Technical Representative (CTR) and Activity Contract Technical Representative (ACTR) Approval**

The requestor/site contacts the site CTR/ACTR to request the release. The CTR/ACTR, using the ISF Tools Database, reviews the request to determine that a deployable solution is available. The CTR/ACTR also determines if funding is available to support the deployment. If the release or funding is found to be unavailable, the CTR/ACTR notifies the requestor/site.

### **3.6.6 Add Application to Rationalized List**

Once the CTR/ACTR has approved the request, the requestor/site updates the rationalized list with the new release. If the rationalized list cannot be updated, the requestor/site notifies the Command and requests an update of the affected rationalized list. If the release replaces an existing application on the site/Command rationalized list, the old application is removed just prior to deployment of new release. This step ensures that the application inventory for the site/Command reflects an accurate inventory of all applications deployed within the site/Command.

### **3.6.7 Complete an Service Request Management (SRM) [Move, Add, Change (MAC)] Form or Distribution CLIN**

The CTR/ACTR completes a MAC form or submits a Distribution CLIN request upon verification that the release is available in the ISF Tools Database for deployment. The MAC form is available at [http://www.nmci-isf.com/helpdesk\\_reqforms.asp](http://www.nmci-isf.com/helpdesk_reqforms.asp). The MAC or Distribution CLIN request notifies



EDS to begin work for deployment of the application. Refer to Paragraph 4.12.1 for information on Service Request Management (SRM).

### **3.6.8 Complete Application Mapping**

The requestor/site follows the release mapping process detailed in [Paragraph 6.6.3.5](#) using the template provided in [Appendix I.3](#). All application mapping requirements are identified to support the deployment of the release to the specified users/seats. NET will perform this process when it is available to support this requirement.

**NOTE:** Application Mapping in NET can only occur if the application currently resides on the rationalized list in the ISF Tools Database for the ordering Command.

### **3.6.9 License Requirement**

COTS applications require some form of licensing and some GOTS have imbedded COTS that require licenses. Government is responsible for ensuring that license and copyright rules, regulations, and laws are followed.

The site/requestor must verify if licenses are needed to deploy the application to all users. If additional licenses are required, the requestor/site must obtain the necessary licenses (from the COTS or GOTS developer/vendor) to ensure compliance with Navy software licensing policy. In some instances, a preexisting license may be available or the upgrade may be covered by an enterprise license.

### **3.6.10 License Verification**

Prior to the submission of the SRM (MAC) or Distribution CLIN request, the CTR/ACTR verifies that all requestor/sites requesting the release have obtained the necessary licenses to support the deployment of the release. The submission of the SRM (MAC) or Distribution CLIN request is placed on hold until all licensing requirements have been satisfied.

### **3.6.11 Submit Completed SRM (MAC) Form or Distribution CLIN**

The CTR/ACTR submits the completed SRM (MAC) Form to the NMCI MAC Desk using the following e-mail address: [mac@nmci-isf.com](mailto:mac@nmci-isf.com). The Distribution CLIN is submitted in accordance with the instructions contained in the CLIN.

### **3.6.12 Perform Limited Deployment Evaluation**

The requestor and EDS have a joint responsibility to determine if a Predeployment evaluation of the release is required to ensure the release properly deploys to the affected sites. This evaluation is similar to Application Release Deployment Readiness Activity (ARDRA) and is performed in a live NMCI environment. In general, only complex releases that require connectivity beyond the desktop should be considered for this evaluation. The end state of the Limited Deployment Evaluation (LDE) is a pass or fail.

#### **3.6.12.1 Conduct Limited Deployment Evaluation (LDE)**

The requestor/site identifies a small number of seats to participate in the evaluation. In case of a failure, small number limits resulting damage to the selected seats, rather than all the seats receiving the release. A small number also allows the Backout Plan to be quickly executed and the affected seats returned to a full operational capability.

The requestor/site provides EDS with information on the affected seats to complete the LDE push from the NOC. The NOC prepares that release and coordinate the push with affected seat users. Once the release has been pushed, the user evaluates the deployment to ensure the release loaded properly and is functional. Any failures or problems are identified and documented.

If the release passes the LDE, it continues to the next step in the process.

### **3.6.12.2 Resolve Failure**

The requestor/site and EDS work together in resolving any failures or problems that resulted from the LDE. The following actions may be taken to resolve a failure:

- If a failure requires reengineering, the release is removed from the process and the requestor/site must contact the developer for development of a Release Management Process solution.
- The failure is resolved without reengineering of the release (i.e., manual configuration) and the process continues.

### **3.6.13 Coordinate Deployment**

Coordination is an essential step in this process to ensure that all tasks have been completed and the release is ready for deployment to the site(s). Effective communication between all participants in the installation process ensures that all requirements are understood and executed. Establishing effective coordination between the requestor/site, CTR/ACTR, and EDS helps to ensure that any problems are identified and corrective action is applied to quickly resolve the problem.

### **3.6.14 Deploy Release to Sites/Users**

The final step in the RRPTE process results in the deployment of the application/release to all affected users. The following release types determine the overall urgency of the release:

- **Routine:** Releases that are on a normal deployment schedule
- **Urgent:** Releases that are needed to address key business drivers (seat rollout, security vulnerability, potential customer outage). The users cannot perform the business function.
- **Emergency:** Releases that address loss of service, degraded service and performance, safety, and/or security attacks. Unplanned releases are initiated by the Command/site and must be approved by the NNWC.

## **4.0 PREPARATION AND ANALYSIS**

This section provides an overview of DON and NMCI policies and requirements that must be considered in developing new releases or changing existing applications. Application of this information during the design and development of the release reduces delays in moving applications through the Testing, Certification, Accreditation, and Deployment processes.

### **4.1 DATA COLLECTION AND ASSESSMENT**

A database catalog lists all applications that have been submitted for deployment in NMCI. This database is maintained by EDS and resides in the ISF Tools Database. The developer is responsible for conducting data analysis to eliminate duplication of effort and to ensure the upcoming application can operate in the NMCI environment. [Appendix E](#) lists the factors used to evaluate applications migrating into NMCI. The developer must obtain FAM approval prior to proceeding with development.

### **4.2 ENTERPRISE RATIONALIZATION**

Enterprise Rationalization is the process of identifying which desktop and server-based applications, both COTS and GOTS, are required to support Command or DON missions, goals, and business processes. It includes the integration, consolidation, and elimination of applications and associated databases; improving standardization; enhancing security; and minimizing support costs. Rationalization policy and guidance is primarily the responsibility of the Deputy CIO (Navy), whereas service-level policy and guidance is the responsibility of the respective Service CIOs. Claimant/Marine Corps-level policy and guidance for rationalization of software applications is the responsibility of the CIO of the claimant/Marine Corps organization.

The DON-level enterprise rationalization process has a structured approach to information management framework; this includes functional and acquisition program managers to ensure horizontal integration (HI) of systems and databases. This process ties into the Enterprise Resource Planning and TFW initiatives. It includes identifying duplicative applications, older versions of applications, and applications that have completed certification, as well as working with the Navy claimants and Marine Corps organizations to resolve issues. FAMs lead this rationalization process.

### **4.3 DEPARTMENT OF THE NAVY APPLICATION DATABASE MANAGEMENT SYSTEM (DADMS)**

To enhance the Navy success in effectively implementing NMCI, the CNO established a goal to reduce Navy Legacy Applications by 95% within one year (by May 2003). To accomplish this effort, the DON CIO directed the development of DADMS.

The DADMS was created as a tool to enable the FAMS to segregate applications by function, identify and catalogue application attributes, and manipulate information related to applications. It is intended to help reduce the number of applications needed to support the operation of the Navy IT enterprise.

DADMS supports the FAMs and FDMs in developing standard applications, databases, and data elements. It provides structure to maintain configuration control of all applications and databases across all DON networks. This helps the integration process to capture both the Navy and Marine Corps existing IT business rules and requirements. Processes and procedures can be found on the Department of the Navy Chief Information Officer DON Application & Database Management System (DADMS) Home Page (<https://www.dadms.navy.mil/>) under “Policy and Guidance.”

## 4.4 FAM PROCESS SUMMARY

FAMs and Command organizations employed short-term and mid-term rationalizations to decide whether to retain or eliminate applications. The short and mid-term rationalizations were iterative processes that employed a questionnaire to score, rate, and categorize applications. Developers and Commands populated the questionnaire. It was then scored automatically to help FAMs decide dispositions and prioritize applications. However, the questionnaire score was only a tool for the FAMs; the FAM made the final decision. In order to make the most reasonable decisions, the FAMs considered Command recommendations, requirements, and all available directives. The FAM high-level decision criteria can be generalized as follows for each application disposition:

- **Approved:** Applications identified as preferred, Gold Disk applications; applications that must be retained for a considerable timeframe; and the most current version, etc.
- **Allowed with Restriction (AWR):** Applications that had sufficient information provided in the questionnaires for FAM to maintain until further analysis could narrow the number of applications with redundant functionality.
- **Disapproved:** Applications that had unknown versions, no POCs listed, missing or incomplete questionnaire information, NMCI Application Ruleset failures, and duplicate records.

FAM Approved and AWR applications are slated for follow-on migration planning, analysis, and execution to identify and implement the “best” software solution for all stakeholders. The “best” solutions will be determined by implementing a business case analysis process, which considers the objectives and priorities of all stakeholders, including the objective to achieve the Navy goal for reducing applications supporting DON functional requirements.

### 4.4.1 Failed Status for FAM Disapproved Applications

In the case of a FAM “Disapproved” application, the ISF Tools Database reflects the following information. Disapproved applications are marked as “Failed due to violation of NMCI Ruleset 13,” which states that the candidate application is personal, nonmission, or nonbusiness related and is therefore prohibited in the NMCI environment. A failure letter is generated to document the assignment of this failed status.

## 4.5 NMCI APPLICATION RULESET

All applications are reviewed against the NMCI Application Ruleset for compliance. Applications found not to be in compliance with the ruleset are subject to FAM waiver, or are killed and removed from NMCI. Not all rulesets are waivable. [Appendix D](#) provides a more detailed explanation of the ruleset requirements.

Developers are encouraged to consider development requirements specific to supporting IT-21, the Marine Corps Tactical Network (MCTN), BLII, and the TFW. The goal is to standardize applications and databases across all networks, if feasible.

## 4.6 FAM APPLICATION WAIVER PROCESS

For any required application that was discarded by the FAM in either short-term or mid-term rationalization, the “owning” Command may submit a waiver. In this scenario, the owner is the site and personnel that requires the application to support business processes and the mission. In most cases, the application requiring a waiver had been disapproved because of lack of information. The FAM process

and the DADMS *mandate* that an application have a populated questionnaire with a unit identification code (UIC) signature, Command signature, and a developer signature in order for the recorded application to be retained in either an Approved or AWR status. Therefore, the owner must identify the application, search for it in DADMS, and have it waived for Command and FAM approval.

Waiver processes and procedures can be found on the Department of the Navy Chief Information Officer DON Application & Database Management System (DADMS) Home Page (<https://www.dadms.navy.mil/>) under “Policy and Guidance.” **NOTE:** The FAM application waiver process should NOT be confused with the waiver submission to the NMCI DAA. A waiver for a port exception is only an interim technical solution process that does not generally involve any FAM interaction.

#### 4.6.1 How to Waiver an Application

The owner must search for the application in DADMS, and it must not be a duplicate record. Once the record is found, the owner must click the waiver button to begin the waiver process. DADMS requires an additional questionnaire specific to the waiver. This questionnaire asks why the application waiver is being requested (i.e., due to an NMCI Application Ruleset failure, quarantine/kiosk status, expired waiver, etc.). All information must be populated in questionnaire steps 1 through 6, if applicable.

The DADMS main page provides assistance in filling out a questionnaire or questions on the FAM process under “DADMS Help.” Additionally, once a waiver is completed, the owner should notify the Command representative to ensure a review of the waiver and to obtain further guidance.

#### 4.7 CERTIFICATION AND ACCREDITATION (C&A)

All DoD information systems that enter, process, store, or transmit unclassified, sensitive but unclassified (SBU), or classified National Security information, including contractor operated or owned facilities under DoD authority, must be certified as meeting minimum security requirements and be accredited for operation by a cognizant DAA. Owners and developers of legacy networks, systems, and applications wanting to transition into or connect to NMCI must document both system engineering activities and supporting security C&A activities to demonstrate to the Navy NMCI DAA that the network, system, or application meets the minimum IA requirements.

Existing Navy systems/applications often have not completed all DoD/DON-required security C&A processes defined in the DoD Inst 5200.40 DoD Information Technology Security Certification and Accreditation Process (DITSCAP) and Department of Navy IA Publications on C&A, the DON IA Pub 5239.13 (Volumes I and II). Many systems/applications were developed or acquired prior to the existence or implementation of the DITSCAP and current Navy IA requirements. Other systems/applications have been provided to the Navy and allowed to operate without supporting security or system configuration documentation. The lack of detailed development information, systems engineering, and security documentation regarding these systems makes it difficult for the Navy NMCI DAA to ensure that transition to NMCI can be accomplished within acceptable IA parameters.

If a system/application requires communications across NMCI boundaries, compliance with minimum IA requirements is essential regardless of CLIN or whether a system/application is hosted and managed by NMCI or the Government. Failure to identify the communications paths and to meet the minimum IA requirements will prevent the system/application from functioning properly.

To ensure that these requirements are fully documented and understood, NNWC, the NMCI DAA, follows the process defined in DoD Instruction 8510.1-M, DITSCAP Application Manual. This document

provides detailed information on the DITSCAP process to assist the developer and Command in completing and submitting documentation for review and approval by the NMCI DAA.

Additional information pertaining to the DITSCAP process and document-generation tool is available at <http://iase.disa.mil/ditscap/index.html>

#### **4.7.1 Purpose**

The DITSCAP applies to C&A professionals, users, acquisition and maintenance organizations, developers, system integrators and procurement officials. Each community has a specific role in developing, procuring, employing, and operating an information system (IS) with an acceptable level of residual risk. These communities perform the following tasks:

- Identify the IA requirements, Level of Effort (LOE), and the C&A approval process necessary for successful deployment to NMCI,
- Define efforts required to ensure compliance with published DoD C&A policies while remaining DITSCAP compliant for existing fielded systems/applications.
- For a system or application in development:
  - Identify security requirements.
  - Design to meet those requirements.
  - Test the design against the same requirements.
  - Monitor the accredited system for changes or reaccreditations as necessary.

#### **4.7.2 DITSCAP Application Manual Objectives**

The objectives of the DITSCAP Application Manual are as follows:

- Assist and guide a developer or local system/application owner in constructing a DITSCAP of the current security posture of the system/application.
- Establish an evolving, yet binding, agreement on the level of security required before the system development begins or changes to a system are made. After accreditation, the DITSCAP becomes the baseline security configuration document.
- Establish a standard process, set of activities, general tasks, and a management structure to certify and accredit that the system or application is compliant with the IA and the security posture of NMCI.
- Support an infrastructure-centric approach, with a focus on the mission, environment, and architecture.
- Define processes that determine current technical details of IA, communications, and architecture associated with systems or applications in their “as-is” environment.
- Provide the guidance necessary to fully satisfy DoD/DON C&A requirements as defined by the NNWC NMCI DAA office.

### **4.7.3 Application and Scope**

The DoD and DON C&A requirements apply to the following entities:

- Navy activities, organizations, contractors, and systems or applications, including all information systems that enter, process, store, or transmit unclassified, SBU, or classified National Security information, whether in Government-owned or contractor-operated-or-owned facilities under Navy authority
- Fielded Program of Record systems/applications that have not been accredited in operational environments
- Systems/applications that meet the requirements for operation within NMCI
- Systems/applications that select CLIN options to deploy into NMCI (CLIN 29)
- Systems/applications or networks that select CLIN options to connect to NMCI but retain some or all administrative and DAA control (CLIN 27 and CLIN 32).

### **4.7.4 NMCI DAA Policy for Certification and Accreditation of Applications on NMCI**

In accordance with COMNAVNETWARCOM message 141945Z Nov 2003 / NIA 11-03, the NMCI DAA provides guidance for the post cutover application release deployment process. Table 3-1 specifies the type of C&A work required to obtain DAA approval. This table provides 12 scenarios to help determine the type of C&A work required to support the release.

The NMCI DAA has instituted the following policy that supports the NRDP for upgrades to existing applications and the introduction of new (emerging) applications in NMCI.

#### **4.7.4.1 Simple Applications**

For simple applications (client/desktop/standalone) being introduced for the first time or being upgraded to a new version, the NMCI DAA issues a three-year ATO upon successful completion of packaging, testing, and certification of security compliance by the Applications Lab. No further C&A work is required for these types of releases.

#### **4.7.4.2 Complex Applications**

For complex applications (client/server) where the server resides outside NMCI and the desktop resides inside NMCI, upgrades to the client portion only require satisfactory completion of EDS packaging, testing, and certification. Upon completion of the certification, a one-year IATO is issued for the client portion, pending submission of required C&A documentation in accordance with DoD Inst 5200.40 and Navy IA Pub 5239.13 Series (as applicable).

## **4.8 INFORMATION ASSURANCE (IA)**

IA is critical to the success of NMCI. Through enforcement of security procedures, NMCI enables users to access information and services with the appropriate security trust necessary to do their jobs. Defense-in-depth protection mechanisms are deployed in a layered fashion, forming boundaries at multiple levels within the security architecture of the desktop and network. These processes ensure resistance to attacks and minimize the possibility of a security breach due to a weakness (known or unknown) at any single security component. Defense-in-depth protection strategies provide security features to NMCI systems



and data and include such features as confidentiality, integrity, availability, accountability, authentication, and nonrepudiation.

## 4.9 SECURITY

### 4.9.1 Boundary Protection

Figure 4-1 depicts a standard set of boundary protection, which has been incorporated into NMCI to protect interfaces within NMCI and other networks. The National Security Agency (NSA) Guide to Securing Microsoft Windows 2000 Networks, as published by the Network Security Evaluations and Tools Division of the Systems and Network Attack Center (SNAC), provides the framework for these protection standards. Boundary protections enforce the policies required to connect to external networks; provide security mechanisms for secure access to applications, and protect COIs residing within NMCI. Section 5.0 discusses this area in further detail.

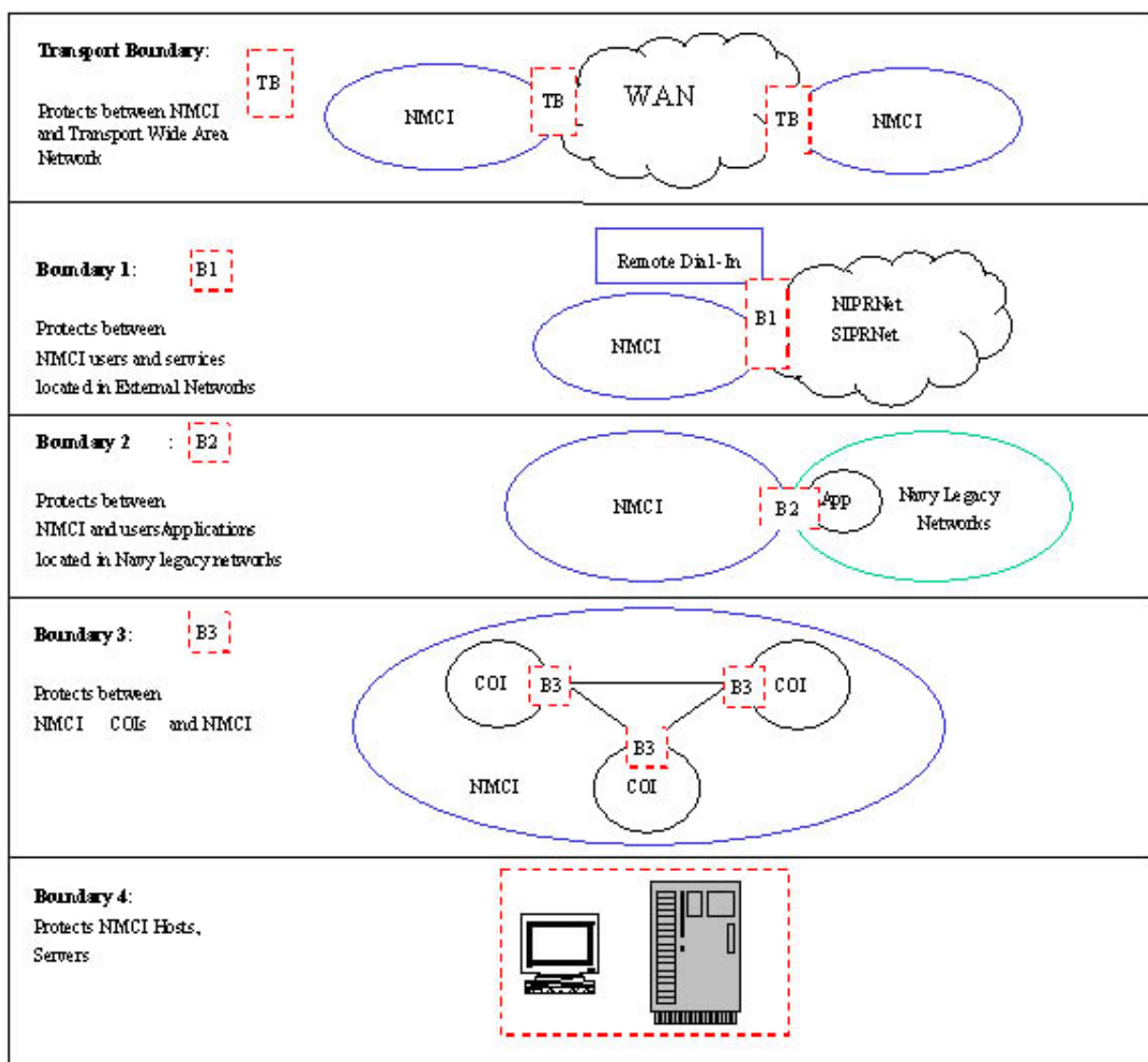


Figure 4-1 Network Boundaries



## **4.9.2 NMCI Public Key Infrastructure & Directory System**

NMCI employs Public Key Infrastructure (PKI) Class 3 certificates for strong user identification and authentication (I&A) and e-mail sign on. Infrastructure components are Public Key Enabled (PKE) for reciprocal authentication. NMCI implementation of DoD PKI provides accountability and nonrepudiation, and to a lesser degree, data confidentiality and integrity.

NMCI is compliant with DoD and DON security policies using two-way SSL and requires the installation of a DoD Class 3 PKI identity certificate on the workstation. Each user must contact the local certification authority to obtain a PKI certificate. Specific DoD implementation of PKI in the Navy can be found at the InfoSec website PKI primer: <https://infosec.navy.mil>.

## **4.9.3 Boundary 1 (B1) Conditionally Allowed Ports**

Typically "conditions" are attached to the use of these ports that are "Conditionally Allowed" on NMCI. All applications that must communicate over the "Conditionally Allowed" ports must adhere to these "conditions." If proper compliance to the "conditions" is achieved, the application is permitted on NMCI (from an operational perspective). That is, the developer does not need to submit a "Request to Operate a Noncompliant System" to Space and Naval Warfare Systems Command (SPAWAR) Program Management Warfare (PMW)-161 for processing through CNO.

The developer or Command must provide sufficient information to the DAA that the application/release will comply with the "conditions" and ensure that EDS B1 firewall administrators understand the conditions. Each application that attempts to use the "Conditionally-Allowed" port must have the following information submitted in order to receive authorization to deploy the application:

- DITSCAP based package.
- Interim Authority to Operate (IATO) letter of recommendation issued by SPAWAR PMW-161 for large PORs.
- POR, or NNWC or local/developer DAA, for smaller systems (non-POR)
- Preexisting IATO submitted to NNWC for review with the C&A documentation.
- The total port, protocol, service, and direction of initiation (P/P/S/DI) requirement for system communications and topology. (Destination Internet Protocol (IP) addresses are required for specific port usage.)

For each legacy application/system transitioning to NMCI using the "Conditionally Allowed" ports, the NMCI DAA maintains a listing/registry to ensure that they have a complete picture of which ports are being used. This listing supports enterprise decisions for Information Assurance Vulnerability Alert (IAVAs), NAVCIRT Advisories, etc.

## **4.9.4 Active Directory (AD)**

Within NMCI, security administration uses the basic features of the AD, groups, and organizational units (OUs). AD is a Microsoft trademarked directory service (DS) that provides the basic security policy enforcement and access control administration mechanism for NMCI. AD, which is an essential component of the Windows 2000 network architecture, presents organizations with a DS designed for distributed computing environments. AD allows organizations to centrally manage and share information on network resources and users while acting as the central authority for network security.

#### **4.9.5 Security Objects: Group Policy Objects (GPOs)**

The GPO enforces the operating system desktop security mechanism. NMCI uses the Windows GPO guidelines for some of its security enforcements. This guide does not include these guidelines; they are available to developers through NNWC and EDS. Paragraph 5.4 discusses this area in further detail.

#### **4.9.6 Security Management**

DON and EDS personnel jointly manage NMCI security, where the DON sets policy and EDS is responsible for implementation. Although the Security Operations Centers (SOCs) are staffed primarily with EDS personnel, the DON exercises Command Authority over EDS defensive Information Warfare activities. Security is managed in compliance with all relevant DoD and DON policies.

#### **4.9.7 Firewall Policies**

As a DoD entity, the Navy is bound by DoD directives, memorandums, instructions, manuals, publications, mandates, etc. that must be adhered to by its networks. In an effort to comply and protect its own information, the Office of the Chief of Naval Operations (OPNAV) has issued the Navy-Marine Corps Unclassified Trusted Network Protection Policy (UTN Protect) that can be found at the DoD PKI certificate enabled security website: <https://infosec.navy.mil>. Information, updates, and status of this policy can also be found at <https://infosec.navy.mil/>. (Authentication is required to access actual policy.) Developers of Navy Enterprise applications that must traverse through Navy network boundaries must familiarize themselves with this policy, ensuring that their applications pass through the boundaries and thereby increasing their chances to expedite testing and obtain application certification.

#### **4.9.8 Desktop GPO Implementation**

NMCI enforces Navy and Marine Corps security policies by facilitating Microsoft AD and GPO functionalities. EDS, through the use of Novadigm Radia manages installation, configuration, and updates to applications within NMCI. NMCI users are not permitted to install software, except on a Science and Technology (S&T) seat. As stated before, Novadigm Radia packages include settings in configuration files, set path variables, icon file location, application drivers, etc. If the release settings violate GPO policy, the developer must reconfigure the release to comply with policy requirements.

#### **4.9.9 File and Registry Permission**

NMCI client images contain file and registry entries that provide appropriate permissions designed to conform to security requirements while allowing most applications to function properly. The following paragraphs describe how these settings affect applications deployed to NMCI clients.

##### **4.9.9.1 File Permissions**

The NMCI user desktop is a single partitioned C: drive; and the client image has special permissions. The GPO only allows users and applications to create folders and files in designated areas of the file structure. The following restrictions apply:

- NMCI seats are set with the NMCI EDS screen saver. The screen saver cannot be changed.
- Users can create subdirectories in the root directory.
- Applications can create subdirectories in the C:\PROGRAM FILES directory during installation.

- All operating system level files (autoexec.bat, System32, etc.) are not available for update by applications. The C:\WINNT directory can be written to or appended, but not overwritten.
- Desktop users may not change application files. Application files are distributed to the user's desktop using the AD, Novadigm Radia, and Gold Disk processes.
- Releases deployed to NMCI clients must be placed in subdirectories below C:\PROGRAM FILES. NMCI requires that release data be stored in the user's "My Documents" subdirectory. The location of the "My Documents" subdirectory should be obtained programmatically because this is not the same for all users / profiles. For example, terminal services users have their My Documents subdirectories redirected to their home subdirectories on the network.

To ensure that NMCI workstations are both secure and stable, users (and applications) are allowed to write only in designated folders on their local hard drive. These permissions are enforced using the Windows 2000 GPO.

#### **4.9.9.2 Registry Permissions**

Registry permissions change periodically. For current registry permissions, refer to the GPO information provided by NNWC and EDS. As with file permissions, Radia can write to all areas of the registry during installation of the application through the system account. However, once the application is installed, the user is restricted to the areas governed by the GPO while running the application. Therefore, the application should be designed to only write to those areas during runtime.

### **4.10 INFORMATION ACCESS & SYSTEM SERVICES**

#### **4.10.1 CLIN**

The NMCI ISF provides services to a range of Navy and Marine Corps end points or service delivery points (SDPs). These SDPs include voice, video, and connection points for end users, general NMCI enterprise, and interfaces to other DON and DoD communications environments. Specific services to be provided to the end points vary but include the IT services listed by CLIN.

#### **4.10.2 File and Print Services**

File and print services are two of the most fundamental services within NMCI. File servers provide secure storage space for both public and private files. Print services allow users to produce black and white, color, or transparent hard copies of work created with NMCI hardware and software. Both services rely on the server platform and are connected to the user through the physical network.

##### **4.10.2.1 User Identification and Access**

For safety, server physical access should be limited to individuals who are experienced network administrators. Authentication Windows 2000 user access technologies authenticate these individuals. If an individual cannot be authenticated, server access is not granted to that server or any services operating on that server.

##### **4.10.2.2 Computer Virus Protection**

NMCI proactively provides virus monitoring at multiple levels within the NMCI infrastructure. Since virus definition, operating system patches, and other updates may occur automatically, the desktop

computer should remain on overnight, with the user logged off, to allow network-managed software housekeeping.

### 4.10.3 Print Services

AD manages the Microsoft Windows 2000 print subsystem and allows a user to query the AD for available printers, as well as the default printer. Application developers should use AD to determine that a printer has the required print capabilities.

### 4.10.4 File Storage Services

User accounts are allocated 1 gigabyte of storage on a file server. Additional public storage can be purchased in 10-gigabyte increments by requesting a Task Order (TO) under CLIN 0016. Storage space is divided as follows:

- **Private:** 700 MB
- **Public:** 100 MB (pooled and controlled at Command level)
- **Growth:** 200 MB (25%)

For account services, each seat (red, white, blue, or deployable) comes with two unclassified accounts. Unclassified user accounts can be aggregated and used to provide unclassified access through existing unclassified NMCI seats.

Table 4-1 lists the available following drive letters and backup routines.

**Table 4-1 Available Drive Letters and Backup Routines**

Drive	Description	Incremental	Full Backup	Shared
C:	My Documents - local desktop. GPO rules are applied	None	None	No
H:	(Home) network directory for a user's private files or storage	Nightly	Weekly	No
S:	(Shared) network directory. Command public files or storage	Nightly	Weekly	Yes

### 4.10.5 File Sharing

EDS implements login scripts to map file shares. Each user has an "H:" and an "S:" drive mapped on a specific machine through a login script. The "H:" drive is the private drive of the user and cannot be shared. The only file sharing exists on the "S:" drive, and that file sharing is limited to the public portions assigned to that specific user. Standard Microsoft file sharing rules and permissions apply. The "C:" or local drive and all of its contents are not shareable. This policy is standard throughout the NMCI environment. Additional shares should be mapped with a drive letter that is consistent across the NMCI enterprise.

Users do not have delete or change permissions and cannot take ownership of files they did not create; nor are they allowed to share private storage or create shares on their desktops. Users should verify that adequate space is available on a network drive before writing files to these resources. Developers must not to remap the public (S) and private (H) network directories.

#### 4.10.6 Personal Storage

Users are assigned a network drive that points to their private data (H:\), and cannot provide shared access. To share files with others, users must use the Command shared network drive space (S:\).

The home drive (H:\) points to a user's personal file space located under the USERS directory on each file server. This space stores files used only by the individual user [e.g., files such as the mail personal storage (.pst) file].

#### 4.10.7 Shared Storage

Within NMCI, shared storage is allocated by Command. Folders and files located in this shared storage permit users to read, write, and execute files. Users may create and delete folders. Designated individuals within the Command may control access to the shared storage. NMCI shared storage is not accessible from outside the NMCI enclave.

The shared drive (S:\) points to group data. Each Command is given a folder containing the shared space for all of its users. The directory is shared at the Command level, and the Command designates which user accounts are made owners of the directory. By allowing the designated owner to control access using New Technology File System [Microsoft](NTFS) permissions, the Command can exercise the greatest level of flexibility over the allocation of this storage space.

#### 4.10.8 File Share Naming Conventions

File sharing follows standard Universal Naming Convention (UNC) paths. Refer to Table 4-2. AD uses the following format for file share naming:

\\CCCCC\LLLL\SSSSSSSS

**Table 4-2 File Share Naming Conventions**

Symbol	Represents	Character Count
CCCCC	Command	Variable
LLLL (Optional) (Local Shares Only)	Site Identifier	Four
SSSSSSSS	Share Name	Variable

##### File Share Naming Examples:

\\SPAWAR\SPOT\Group161  
\\MARFORPAC\PLMS\SOFTWARE  
\\NAVAIR\PAXR\ADMIRALS SHARE

#### 4.10.9 Printer Naming Format

Printer names may be up to 80 characters long. The standard NMCI printer driver is Postscript. Refer to Table 4-3. AD uses the following format for network printers:

\\LLLL\BBBBBB\FF\RRRR\OOOOO

**Table 4-3 Printer Naming Format**

<b>Symbol</b>	<b>Represents</b>	<b>Character Count</b>
LLLL	Site Identifier	Four
BBBBBB	Building Identifier	Variable
FF	Floor Identifier	Variable
RRRR	Room Identifier	Variable
OOOOOO (Optional)	Printer Identifier	Variable

Printer Naming Examples:

\\PAXR\Bld6\02\28\HPLJ5  
\\FALL\B421\01\02\HPLJ5  
\\MRMR\BLD5\01\331\HPDJ740

#### **4.10.10 Messaging and Collaboration**

NMCI messaging uses the Microsoft Exchange 2000 suite. The following paragraphs explain the system services of this suite.

##### **4.10.10.1 E-Mail Addressing**

###### **User Principal Name (UPN)**

E-mail addressing within NMCI use the UPN format that follows industry-accepted Simple Mail Transport Protocol (SMTP). A UPN is a multivalued attribute of each user object that the system administrator can set. UPN allows the underlying domain structure and complexity to be hidden from users. For consistency, the UPN and SMTP address format are identical.

The UPN is unique across NMCI. The naming convention has been adopted as follows:

- Firstname.lastname@service.mil (where service represents Navy or Marine Corps)

In the case of multiple users with identical names, the following additional conventions are used to establish uniqueness in the order of precedence:

- Firstname.m.lastname@service.mil where m represents middle initial
- Firstname.m.lastname#@service.mil where # represents a unique numeric identifier starting at 1.

Examples of UPNs for several Joe Users are:

joe.user@navy.mil  
joseph.user@usmc.mil  
joe.k.user@navy.mil  
joe.k.user1@usmc.mil  
joe.k.user2@usmc.mil

##### **4.10.10.2 Mail-Enabled Public Folders**

To allow multiple users access to a common mailbox, mail-enabled public folders have been implemented. These folders appear in the global address list as a mail recipient for Microsoft (MS)

Outlook clients. Users that require this access are granted the appropriate e-mail permissions (view, send as, etc.). See the Microsoft Developer Network (MSDN): <http://msdn.microsoft.com/>.

**CAUTION:** Not all features are available within the NMCI security model. Developers must understand the restrictions implied by group policy and lockdown in order to determine which features are available.

## 4.11 PLATFORMS

### 4.11.1 Client Seat

NMCI client seats are EDS-managed seats. Therefore, users do not have administrative rights to desktop configuration or software installation. The basic client seat is delivered loaded with the latest standard Gold Disk configuration. Additional components can be installed on a client; however, an administrative facility pushes these to the seat. End users cannot add software to their seat;

**IMPORTANT:** Content developers should verify that client plug-ins and components are available and compatible.

#### 4.11.1.1 NMCI Standard Desktop Configuration CLIN 0001-0004

The [CLIN Service Matrix](#) provides numerous options for standard desktop configurations. This matrix contains detailed information on the seat services and the Service Level Agreements (SLAs) included with various seats. Additional information on the desktop CLINS is available at <http://www.nmci-isf.com/clinlist.htm>.

**IMPORTANT:** Developers should consider peripherals when developing an application. They should consult the Microsoft Compatibility List.:

<http://www.microsoft.com/windows2000/server/howtobuy/upgrading/compat/>

As long as the peripheral has a Windows 2000-compatible driver (either from Microsoft or from its own manufacturer) and it does not violate any IA rules or SLAs, it should be able to transition into NMCI.

Legacy desktop single-user devices should transition with no additional fees as long as they are "plug & play". Legacy network multiuser devices need a CLIN 29 request.

The following NMCI standard desktops are available:

- Fixed Work Stations: Red, White, Blue, and Thin Client
- Portable and Ultralightweight Portable Seats
- Embarkable Work Station: Full Service and Limited Service
- Embarkable Portable Seat : Full Service and Limited Service

### 4.11.2 Science and Technology (S&T) Seat

This seat upgrade accommodates the special requirements of the S&T community by allowing the end user to reconfigure hardware and software without EDS intervention. This seat employs architectures and policies that are in accordance with the NMCI EDS security requirements. Customer support is limited to those services offered by EDS and not extended to software or hardware loaded and configured by the user. EDS is not responsible for SLA performance directly impacted by these seats due to the associated relaxed CM policies. The S&T desktop provides the latitude for those who need a software development



platform and the ability to access settings and file locations that are restricted on normal NMCI seats. To order an S&T seat refer to CLIN 0038AA-AH.

The S&T seats provide the following characteristics:

- Allow rapid hardware reconfiguration
- Allow collaborative work and data-file sharing
- Allow software to be personally loaded to the desktop
- Connect to non-Windows 2000 operating systems (Solaris V8)
- Support nonstandard protocols
- Meet high bandwidth requirements
- Provide appropriate security mechanisms

S&T seats reside behind the Boundary 3 (B3) firewall, which protects the NMCI. Further information about S&T seats can be found at [http://www.nmci-isf.com/userinfo\\_sandtguide.htm](http://www.nmci-isf.com/userinfo_sandtguide.htm). A detailed description of the CLIN list can be found on EDS web site at <http://www.nmci-isf.com/clinlist.htm>.

Developmental seats require elevated user privileges, including installing, removing, and compiling code. Because of this elevated privilege and increased risk potential, the developer community was placed in a COI to separate it from the normal user community. This protects the bulk of NMCI users from the elevated risk, while permitting the developer community to perform application development.

The NMCI DAA has delegated the responsibility of deciding what software or hardware is loaded to seats within the developer community to the local DAA. This could be the commanding officer (CO), officer in charge (OIC), decision height (DH), or PM lead of the unit/division/workshop/program. The S&T user communities are given "keys to the kingdom" (access to the basic seat configuration) so they can manipulate their S&T seats as required. The Navy NMCI DAA expects local DAAs to be responsible for conducting themselves within their professional roles, to include installing or deleting applications within their development communities. EDS is not going to install applications on S&T seats other than initial loadout, which is the Gold Disk plus CLIN options, and perhaps part of a rationalized list. The user is responsible for any changes to the S&T seat after the initial loadout. If the installed development software impedes the ability of the user to access NMCI services (mail, print, file shares, etc.), the user is responsible for rebuilding or reloading to initial specifications and starting over. Alternately, a user could call the NMCI Help Desk and risk a MAC charge if the problem was not an EDS issue with basic services.

#### **4.11.2.1 S&T Seat Precertification**

As an interim measure until the Precertification CLINs are available, an S&T seat can be configured and used to support release Precertification testing. S&T seats have a relaxed GPO that allows the user administrator rights to load the necessary software required to perform this function. At a minimum, the S&T seat must be configured with the latest version of the NMCI Gold Disk load set, the current version of the NMCI seat GPO, Windows 2000, and appropriate software that monitors and collects data on the ports, protocols, and services used by the release.

The developer must follow all prescribed Precertification requirements contained in [Paragraph 6.5.4](#). The following steps are performed as part of this process:

1. Ensure the S&T seat is properly configured to support Precertification testing.



2. Install a clean version of the release media on the seat. This also includes any dependent or supplemental media required for the release to operate properly.
3. Run the application and verify that it operates when supported by the Windows 2000 operating system and that it does not break or otherwise alter the operational capability of the Gold Disk load set.
4. Verify the desktop security and ensure the release interfaces with and is compliant with the NMCI GPO standard.
5. Capture the ports, protocols, and services used by the release for network connectivity. The developer should know both the outbound and inbound ports and protocols used by the release.
6. Document results of the Precertification test and include them in the RDP.

#### **4.11.2.2 NMCI S&T Desktop Configuration CLIN 0038**

This seat upgrade accommodates the special requirements of the S&T community by allowing the end user to reconfigure hardware and software to without EDS intervention. This seat employs architectures and policies that are in accordance with the NMCI ISF security requirements. Customer support is limited to those services offered by EDS and not extended to software or hardware loaded and configured by the user. EDS is not responsible for SLA performance directly impacted by these seats due to the associated relaxed CM policies. More detailed information on S&T seats configuration and available options is available at <http://www.nmci-isf.com/clinlist.htm>

#### **4.11.2.3 Use of Personal Digital Assistant (PDA) Applications Within NMCI**

PDAs are approved for use within NMCI. The CLIN 023 catalog lists the Palm 515 and the Tungsten E. The NMCI DAA intends to issue a type accreditation for the applications that reside within the Palm operating system. This includes the applications that are preloaded “out of the box” and include the *Documents to Go* software (MS Word, MS Excel, and PowerPoint). The NMCI DAA will handle Palm add-on and custom applications that reside on an NMCI PDA on a case-by-case basis. The packaging, testing, certification, accreditation, and deployment of these applications follow the existing NRDP, as explained in Section 6.0. Refer to COMNAVNETWARCOM message R 051645Z DEC 03.

PDA policies in a series of NMCI Information Advisories (NIAs), NMCI Information Bulletins (NIBs), and Naval messages govern PDA usage within NMCI. Presently, Bluetooth and 802.11 wireless technologies are not allowed within NMCI. To ensure NMCI network protection, when the NMCI DAA will allow wireless connections for e-mail and other services on a NMCI PDA device is undetermined.

Sites/Commands requesting a new palm application must use the RRPTE process contained in Section 3.0 to determine if the required application is already available in the ISF Tools Database Application Catalog or through CLIN 23. In the event the required application cannot be obtained through the RRPTE process, the site/Command needs to introduce the application as a new (emerging) application through the NRMP.

### **4.12 NMCI APPLICATION SERVICES**

This paragraph describes services available to developers as part of NMCI. Additional development services may be added over time. This guide will be updated as services are added.

### 4.12.1 Service Request Management (SRM)

The primary objective of SRM is to provide a uniform environment where all NMCI orders are processed timely and records of all changes are maintained. SRM accomplishes this by the following:

- Provides timely and accurate data
- Strictly enforces Enterprise data standards and business rules
- Streamlines dataflow
- Standardizes data access
- Facilitates access to commonly used Enterprise data
- Improves quality, completeness, and consistency of data values
- Improves data access speed
- Eliminates costly, time-consuming, and error-prone manual data handling
- Facilitates reporting

Developers use the service request for the Certification CLIN to support the certification of their application release. Additionally, developers use a service request (MAC or Distribution CLIN) to support the deployment of their release. Application developers ***must*** work with their CTR/ACTR for service request submittal. (A CTR/ACTR is a designated person on the MAC Authorized Submitter List.) A description of the service request process follows.

#### 4.12.1.1 Certification CLIN

Before EDS begins processing a release through Testing and Certification, the application developers' CTR/ACTR must complete a service request for Certification and submit it to the SRM Team. The SRM Team validates the request to ensure that the release is FAM approved, the request is filled out properly, and a CDA RFS is entered into the ISF Tools Database.

Once the service request has been validated, the SRM Team creates a Remedy Ticket. The Remedy Ticket is routed to the Applications Team to prepare for testing once the Applications Lab receives the Application Submission Packet. Refer to Paragraph 6.6.2.

#### 4.12.1.2 Deployment Service Request [Move, Add, Change (MAC) or Distribution CLIN]

For NRDP deployment, the application developer is required to use either of two methods:

- For individual or small numbers of NMCI seats, use a MAC.
- For large numbers of NMCI seats, use a Distribution CLIN.

The application developers' CTR/ACTR must submit this service request to EDS 30 days prior to completion of Testing and Certification. Failure to submit the deployment service request by the deadline will delay application deployment to the seats.

Normally, the application release is packaged (Radia) for electronic deployment into NMCI and is supported by either an administrative (Admin) MAC or a Distribution CLIN. If the application release cannot be packaged for electronic deployment, the only method available is to use a Physical MAC.

Once the service request has been validated, the SRM Team creates a Remedy Ticket. The Remedy Ticket is routed to the Applications Team to prepare for deployment after the application has been certified and ECCB approved.

For information about Site/Command-requested deployment of an application release, refer to the RRPTE process, Paragraph 3.6. More detailed information on administrative MAC options is available at <http://www.nmci-isf.com/clinlist.htm>

#### **4.12.2 Gold Disk**

The NMCI Gold Disk contains standard desktop products and services to be installed on every NMCI client machine. Contents of the Gold Disk are updated as NMCI evolves and are managed through the NMCI Change Control Process. A review of the latest Gold Disk contents is available at [http://www.nmci-isf.com/downloads/Gold\\_disk\\_contents.pdf](http://www.nmci-isf.com/downloads/Gold_disk_contents.pdf)

#### **4.12.3 NMCI Server Connectivity CLIN 0027**

Application server connectivity is a service that provides NMCI connectivity to legacy application servers for Navy and Marine Corps organizational, operational, and functional applications to meet mission requirements. This service meets peak network loading requirements of users for replication, but does not include server and database maintenance and administration. More detailed information on the various server connectivity options is available at <http://www.nmci-isf.com/clinlist.htm>.

#### **4.12.4 NMCI Legacy Systems Support CLIN 0029**

Legacy Systems Support provides initial integration services for emerging operational and functional systems to enable them to run on NMCI. Legacy System Support can also provide additional services beyond basic integration. These additional services provide a range of options that include, but are not limited to, NMCI EDS hosting of applications, operations, and maintenance support; database management; and training, if ordered. This service may include participation of the NMCI EDS in business process reengineering activities. These items are separately priced in individual orders and can be applied to legacy systems that have been integrated to run on NMCI as part of basic service during initial NMCI implementation. Future options will be available under this CLIN to support certification and Precertification of releases in support of existing applications, and for new (emerging) releases being introduced into NMCI for the first time. More detailed information on Legacy Systems Support is available at <http://www.nmci-isf.com/clin029.htm>.

### **4.13 COMPONENTS**

Components are reusable programs that can be used as building blocks with other components to provide common services when building an application. Only standard Windows 2000 Professional components are provided in the NMCI Gold Disk.

### **4.14 DIRECTORY AND REGISTRY PERMISSIONS**

Releases must be written in accordance with MS Windows 2000 standards to ensure compliance with Navy certification standards. In some cases, the DON establishes specific permission standards that must also be included in the release.

Information on Microsoft directory and registry permissions is available at <http://www.microsoft.com/windows2000/>. For information on Navy/Marine Corps specific permissions, contact the NMCI Help Desk.

## **4.15 BROWSERS**

### **4.15.1 Microsoft Internet Explorer Version 5.0 or Greater**

#### **4.15.1.1 Plug-ins Provided on Gold Disk**

The current set of plug-ins provided by the Gold Disk is available at [http://www.nmci-isf.com/downloads/Gold\\_disk\\_contents.pdf](http://www.nmci-isf.com/downloads/Gold_disk_contents.pdf).

EDS is evaluating additional plug-ins for inclusion in the NMCI Gold Disk. Appropriate plug-ins will be included in future releases of the Gold Disk. The Novadigm Radia server may also push plug-ins to desktops.

#### **4.15.2 Netscape Communicator 4.76**

Netscape is included on the NMCI Gold Disk. It is provided as a service for compatibility with existing systems and is not supported by NMCI. All new (emerging) applications should be developed to support the NMCI default browser, Internet Explorer (version 5.0 or later) unless constrained by international treaty or other business requirement to use Netscape.

#### **4.15.3 Browser Security**

NMCI implements the DoD Mobile Code policy. The DoD Mobile Code Policy defines the categories of mobile code and provides criteria for use within the DoD.

The policy is available at <http://iase.disa.mil/policy.html>

## **4.16 EMULATION**

### **4.16.1 Terminal Services**

From a developer's perspective, the Microsoft guidelines are the recommended standard for how to design and construct applications to run in a "multiuser environment," such as an environment with terminal servers.

Microsoft guidelines for Optimizing Applications for Windows 2000 Terminal Services and Windows NT Server 4.0, Terminal Server Edition are available at <http://www.microsoft.com/technet/>

#### **4.16.2 Product Supported**

Reflection is the de facto standard terminal emulator that is included on the Gold Disk and is a standard application included on every NMCI seat. Reflection supports IBM, Hewlett Packard (HP), UNIX, Open Virtual Memory System (VMS), and X Suite environments.

## **4.17 INTEGRATED SOLUTION FRAMEWORK (ISF) TOOLS DATABASE REGISTRATION**

When ready to start the approval process for a desktop application, the developer must enter the application into the ISF Tools Database, which is the current authoritative source for NMCI applications. Only developers may enter new (emerging) applications.

The ISF Tools Database is available at <http://www.nmci-isf.com/transition.htm> (transition link) or <https://usplswebh0ab.plano.webhost.eds.net/isftool/Login.jsp> (direct link).

#### **4.17.1 ISF Tools Database Description**

Application developers/owners must obtain an ISF Tools Database developer account and submit a CDA RFS to ensure that their releases are listed and available for certification for NMCI according to Navy enterprise standards and EDS. The goal is to ensure that applications are necessary (rationalized), appropriate, and can function within the NMCI environment. Once ISF Tools Database access has been granted, developers can access the database to perform their duties. These duties include checking certification testing, viewing application survey data, adding additional applications, submitting applications, and viewing reports, based on the level of access granted by the Command POC.

For more information, application developers should download and review the ISF Tools Database User Manual on the Splash page of the ISF Tools Database or contact the ISF Tools Database POCs. See EDS POCs in [Appendix C](#) for further assistance.

NMCI customers can call, e-mail, or fax messages to the NMCI Help Desk and receive assistance 24 hours a day. Personnel using e-mail are encouraged to direct inquiries to the Help Desk center closest to them: Norfolk, VA, or San Diego, CA.

Phone	1.866.THE-NMCI
Fax	1.877.FAX.NMCI
Norfolk E-mail	<a href="mailto:HelpDesk_NRFK@nmci-isf.com">HelpDesk_NRFK@nmci-isf.com</a>
San Diego E-mail	<a href="mailto:HelpDesk_SDNI@nmci-isf.com">HelpDesk_SDNI@nmci-isf.com</a>

### **4.18 NMCI HELP DESK SUPPORT**

#### **4.18.1 Level 1 NMCI Help Desk Support**

The NMCI contractor is responsible for Level 1 NMCI Help Desk Support.

##### **4.18.1.1 Global Outreach**

NMCI Help Desk agents are located in state-of-the-art network operations centers in Norfolk, VA, and San Diego, CA. Supported by advanced call center automation technology, the agents are equipped to field NMCI user inquiries from across the globe.

##### **4.18.1.2 Personalized Service**

NMCI Help Desk services are available to support classified and unclassified data seat holders 24 hours a day, seven days a week, and 365 days a year.

NMCI Help Desk agents are qualified and ready to resolve any of the customer issues outlined below. Other members of EDS are also available to answer general questions about the NMCI program, address site-specific issues, or escalate persistent problems for resolution.

#### Technical & Application Support

- Problem resolution
  - Laptop (including network connectivity)
  - Workstation (including network connectivity)
  - Software
  - Printer
- Application support
- Password resets

#### Business Support

- MAC requests
  - Process and execute approved user requests
- User account services
  - Create
  - Modify
- Data seat hardware requests
  - Deinstall
  - Move and reinstall
  - Change
- CLIN requests
  - Acquire
  - Install
- Seat upgrade requests

#### **4.18.1.3 Level 1 NMCI Help Desk Support to the Application/Release**

The contractor-provided NMCI Help Desk support is restricted to determining whether the client or network is the cause and then remediating the problem, if possible.

If neither client nor network is determined to be at fault, the NMCI Help Desk agent performs further application troubleshooting, as dictated by developer-provided procedures. If the problem persists, the customer's trouble ticket is escalated to Level 2 support.

#### **4.18.1.4 Developer Support to the NMCI Help Desk (Level 1)**

The developer or application owner should provide the Level 1 NMCI Help Desk with initial troubleshooting questions to perform immediate issue-resolution remediation on the application.

#### **4.18.2 Level 2 and Higher NMCI Help Desk Support**

The developer or application owner is responsible for Level 2 and higher NMCI Help Desk support. Level 2 NMCI Help Desk support should be coordinated with the NMCI contractor providing Level 1

support. For example, Level 2 NMCI Help Desk POCs should be available to the Level 1 agent for immediate customer referral.

#### 4.18.2.1 NMCI Help Desk Manuals

NMCI Help Desk Manuals include the following documentation:

- System Administrator's Manual
- User Manual
- Software Version Description
- Installation Procedures
- System Administrator's Manual

##### User Manual

The User Manual is intended to provide the end user with the information needed to operate the software application. An updated version of this document may not be required for every release of the software application if the contents of the release are only fixes to known issues.

The User Manual has the following sections:

- **Software Inventory:** Lists all components that comprise the software application.
- **Environment and System Configuration:** Provides details.
- **System Overview:** Provides the operator with the main concepts of the software application. This section should briefly describe the Concept of Operations if a separate document has not been developed.
- **Referenced Documents:** Includes any standards (Government and Industry), operational documents, technical documents, and any other documents that are related to the software application.
- **Security Requirements:** Clearly identifies requirements for all aspects of the software application.

The operating instructions for the software application provide keystroke instructions to the user. The instructions cover all software modules and are organized according to common usage or accomplishing specific tasks in the software.

##### Software Version Description

The Software Version Description document provides information specific to the version of the software being released. The information provided focuses on the changes to this version of the software application from the previous. Information in this document includes Software Inventory, overview of the functionality of the released software, Installation Instructions, Referenced Documents, Environment and System Configuration, Security, and known issues. This document is required for every release of the software application.

## **Installation Procedures**

The Installation Procedures is intended to provide the installer with all information required to successfully install the software application. Information in this document includes System Overview, Software Inventory, Hardware Requirements, Installation and Uninstall, Instructions, Configuration and User Registration Instructions, Referenced Documents, Environment and System Requirements and Configuration, and Security Requirements. Additional instructions are provided to the installer to verify the software application is installed, configured, and operating correctly. This document is required for every delivery of the software application.

## **System Administrator's Manual**

The System Administrator's Manual is intended to provide all information required by the system administrator of the software application to manage the application. Information in this document includes System Overview, Referenced Documents, System Administrator Utilities, Operation and Maintenance Procedures, and Error Recovery utilities. This document references the Installation Procedures and User's Manual for information that may be needed to conducted administrator functions. It provides detailed procedures for all maintenance and operating utilities. These include day-to-day operations, security procedures, and backup and recovery. This document is delivered for every version of the software application released.



## 5.0 DESIGN AND DEVELOPMENT

This section focuses on specific requirements an application developer must follow to ensure the release is compliant with NMCI standards. The objective of this guide is not to tell a developer how to develop a release, but to provide the essential information to support the Certification and Testing processes covered in Section 6.0. It also provides information on the different types of release deployments and to support each deployment scenario.

### 5.1 STANDARDS/PROGRAMMING PRACTICES

The NMCI architecture is designed to deliver an integrated family of networks, servers, and workstations configured to support the DON vision for seamless data connection. Therefore, the applications that reside on NMCI must be developed to comply with this architecture and standards.

#### 5.1.1 Microsoft Development Standards

MS Windows 2000 application specifications are used in the development of releases hosted on NMCI in order to leverage the new technologies in MS Windows 2000, make releases more manageable and reliable, and reduce development costs.

Development Standards have two versions:

- **Desktop Specifications:** Refer to <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli.asp>
- **Server Specifications:** Refer to <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2ksrv/html/w2kserve.asp>

This document details the requirements for desktop applications. The application must be compliant with the Windows 2000 installer service to ensure that the application can be cleanly installed/uninstalled, self-repaired, and rolled back on demand.

#### 5.1.2 Programming Guidelines

Adhering to Microsoft guidelines ensures that applications run efficiently within NMCI. Microsoft provides the following specific tuning and optimization guidelines:

- Support Customization Through User Profiles
- No Memory Leaks
- Do Not Replace System Files
- Do Not Assume Computer Name or IP Address Equates to Single User
- DCOM Support
- Consider the Peripheral Hardware Environment
- Do Not Assume Persistence of Files in Temp
- Disallowing Multiple Instances of Some Applications
- Do Not Assume the Windows Shell
- Do Not Modify or replace the MSGINA.dll

- Negotiate Client/Server Connections Inside the System and Network
- Multilingual and International Usage Scenarios

## **5.2 PROGRAMMING STANDARDS FOR A TERMINAL SERVER PLATFORM**

For applications to work well in a multiuser environment, certain programming standards must be used. Terminal servers host applications for multiple end users, but the application must be written so that user-specific information is not tied directly to a machine. For example, applications cannot use the Transmission Control Protocol/Internet Protocol (TCP/IP) address to uniquely identify a user because many users on a terminal server share the same address. Microsoft provides guidance on the following categories:

- Building a Terminal-Services-Aware Application
- Application Setup in a Terminal Services Environment
- Storing User-Specific Information
- Kernel Object Name Spaces
- IP Addresses and Computer Names
- Client/Server Applications
- Graphic Effects
- Peripheral Hardware
- Background Tasks
- Thread Usage

## **5.3 USER INTERFACE SPECIFICATIONS**

Developers must consider user interfaces to applications to ensure that they meet current DoD policy, procedures, and standards (e.g., Defense Information Infrastructure Common Operating Environment - DII COE, C4ISR-AF, DITSCAP, and Section 508).

## **5.4 GROUP POLICY OBJECT (GPO)**

The DON provides a layer of computer defense and control at the desktop by restricting access to the root and system directories, also known as NMCI Boundary 4 (B4) security. In other words, the desktop is “locked down.” The Navy sets GPO settings and policies and EDS implements them. In addition, EDS enforces contract SLA for the desktop by restricting certain user operations and desktop actions.

EDS administers the desktop and application authentication standards. Developers need to contact NNWC or EDS when creating or modifying applications for all GPO related issues. The following guidelines must be adhered to:

- Developers cannot update their Group Policy settings, either locally on the desktop or nonlocally at the AD level.
- Developers must modify releases to comply with GPO policies.
- Developers must go through recertification processes if their releases fail certification testing (GPO testing).
- Developers need to produce test plans/scripts that include the steps, data, and logical conditions necessary to trigger required authentication processes [e.g., Lightweight Directory Access

Protocol (LDAP), AD, file sharing, file writes, etc.] to ensure that group policy, lockdown, and security areas are thoroughly examined during Certification in the EDS Applications Lab.

Releases may be permitted to run as a higher credentialed user. This allows the release to run at a user ID level that has the required GPO/security levels necessary, not as an individual user. Developers are required to program the command set, i.e., run as >userID, and incorporate this in the production environment (e.g., script, .bat file, etc.).

## **5.5 APPLICATION TESTING GUIDELINES FOR DEVELOPERS**

The Applications Lab has developed a set of guidelines for developers to follow when designing applications. The guidelines are based on the Applications Lab experience in dealing with GOTS applications in the NMCI Environment. Guidelines are intended to improve the standardization of GOTS applications, with the following benefits:

- Increase the application compatibility within the NMCI environment
- Facilitate enterprise packaging.
- Reduce certification processing and troubleshooting time

Standardization is organized into three categories:

- Do's
- Don'ts
- Recommendations.

### **5.5.1 Do's**

The Applications Lab requests that developers adhere to the following guidelines in order to significantly reduce the turnaround time of Packaging and Certification.

- Install applications in the C:\Program Files\Application Name folder, where Application Name is the name of the program.

EXAMPLE: Install the program to C:\Program Files\USN AMP, where "United States Navy Aircraft Maintenance Program" is shortened to USN AMP. Support files may be installed to other locations, but the main application must be installed in the Program Files folder.

- Store temporary files in the C:\Program Files\Application Name\Temp folder.

The C:\Temp folder, although traditionally a common location to store temp files, is not supported in the NMCI environment due to its use of the enterprise software distribution system. Temporary files must reside in a location in which users have NTFS write or modify permissions. This temp folder within the application folder allows EDS personnel to quickly identify temporary files when troubleshooting.

EXAMPLE: "C:\Program Files\USN AMP\Temp"

- Store configuration files (e.g., ini, cfg, sys, etc.) in either of two locations depending on the file protection/permission needs.

Locating files in one of these two locations allows EDS personnel to quickly process applications for Packaging and Certification.

- Store files that must or may be updated in the C:\Program Files\Application Name\Config folder.

This unsecured folder allows applications to update the files during run-time.

EXAMPLE: “C:\Program Files\USN AMP\config.cfg” (modifiable at runtime)

- Store files that require a secured folder to prevent modification in C:\WINNT\System32\Developer\Application Name

The secured folder prevents users from changing the files; however, it also prevent applications from making changes.

**NOTE:** This is for files that do not need to be modified.

EXAMPLE: C:\WINNT\System32\Developer\USN AMP\config.cfg” (not modifiable at runtime)

- Store data files (including saved data files and databases) at either the Local Machine or a shared folder in the network.

- **Local Machines:**

- **Single User:** Only one specific user may store and use these files. Store these files in the “My Documents” folder.

EXAMPLE: C:\Documents and Settings\username\My Documents\USN AMP\Data

- **Multiple Users:** More than one person may use these files, which usually serve as a common source of data. Locate these files in the “C:\Program Files\Application Name\Data” folder.

This allows EDS personnel to know where the application data files are stored and take proper measures to prevent those files from being updated or overwritten by the enterprise packaging system.

EXAMPLE: “C:\Program Files\USN AMP\Data”

- **Shared Folders:** Use any shared path as long as the UNC discussed in this document is adhered to.

EXAMPLE: “\\SPAWAR\SPOT\CMDSHARE\USN AMP\DATA”

- Install Application Shortcuts to the “C:\Documents and Settings\All Users\Start Menu\Programs\Application Name” folder.

This ensures that the shortcuts are created in the Start Menu for all users and standardizes the location of shortcuts. The icon (.ico file) of the shortcuts can be of anything ‘nonoffensive’, but should not be the default Windows icon used when a file cannot be found. If an install package that installs shortcuts is used, care should be taken to ensure that only the “All Users” Start Menu shortcut is used.

EXAMPLE: “C:\Documents and Settings\All Users\Start Menu\Programs\USN AMP\USN AMP.lnk”

- Provide test data with test plan for the application if data files (such as databases) are used.

This allows for EDS personnel to conduct tests and be made aware of how the program should function correctly. Based on known test data inputs to the application, known outputs should be generated to ensure that the application functions properly.

- Verify the .msi package using a test program, such as ORCA.

This affects MS Windows Installer (.msi)-based applications; e.g., applications that use the MS Windows Installer and have files ending with .msi file extension the enterprise packaging system cannot correctly package invalid .msi-based applications.

- Create a test login account and a password for applications that require the use of a login.

If a test login account has not been provided, the Applications Lab rejects applications, as the certification test cannot be completely performed.

- Provide the License and/or Registration keys if the application requires their use.

Without the information for those keys, the Applications Lab rejects the application, as the certification test cannot be completely performed.

- Completely fill out the RFS form for each application.

See instructions for this form at the ISF Tools Database Users Guide on the ISF Tools Database Log-in page.

The POC listed should be someone highly familiar with all aspects of the application.

- Provide a copy of the application manual or documentation to ISF personnel on how to take the following actions:

- Install the application.
- Test the application.
- Operate the program.

- Provide an abstract (overview) on what the application is and does.

- Provide information (release notes) on known or acceptable errors and bugs.

Any undocumented error that EDS personnel cannot solve would cause the Applications Lab to reject the application.

- Ship the applications on 3.5” floppy diskettes or CDs.

### 5.5.2 Don'ts

This section lists items that would cause the Applications Lab to reject the applications, or require substantial increased processing and turnaround time for application certification. The Applications Lab

strongly recommends following this list to avoid immediate rejections and shorten the time for certification.

- Do not use desktop shortcuts (shortcuts that are on a user's desktop screen). Desktop shortcuts created from applications are kept to a minimum in the NMCI environment. Users are allowed to create shortcuts themselves.
- Do not compress or zip the preinstalled application. Applications should be installed from diskette(s) or CD(s) without the need to uncompress or unzip. This is because machines used to package the application for enterprise deployment are not able to uncompress or unzip.
- Do not use the term "Beta" for versioning. An application that contains "Beta" in its version is automatically rejected, as this application is assumed to be a preproduction version.

EXAMPLE: Use the numeric format for versioning (i.e., 2.00.2), instead of words (i.e., 2.00 Beta).

- Do not use modems. Do not include any functionality that requires the use of a modem.
- Do not support "Uninstall" or "Rollback" in the installation file executable. The NMCI enterprise application management system handles uninstall and rollback.
- Do not duplicate any Gold Disk applications or their functionality within the release:  
[http://www.nmci-isf.com/downloads/Gold\\_disk\\_contents.pdf](http://www.nmci-isf.com/downloads/Gold_disk_contents.pdf).

### 5.5.3 Recommendations

The Applications Lab provides the following tips to allow for quick certification and ease of troubleshooting or updating.

- Use good design programming standards and practices.
- Provide as much clear information as possible about the application. More information means an easier certification.
- Application configuration files should be in text format. Text-based configuration files allow for quick turnarounds in reconfiguring and preclude a complete repackaging of the application for enterprise deployment.

EXAMPLE: An application designed for use at NAS Pax River is requested for use at NAS Lemoore, and is configured on a network. If the application uses a text-based configuration file, the Applications Lab can make the changes needed to the file within the NAS Pax River package without having to repackage and test the application. If the application has hard coded or embedded files in the application or encrypted, the program must be completely repackaged and certified.

The nature and importance of the application determine how the developer uses the configuration files.

- Minimize the size of the application on local machines. (The developer must determine what is "small" or "large".) For a large application, two possible solutions may be used:

- Use servers to support large programs or files (preferred solution).

For example, a local machine (front end) has a small program to allow a user to use the large database (back end) on a server.

- Use CDs either in a CD library (where possible) or on local machines (least preferred).
- Review the latest GPO revisions. Obtain the GPO information from the NMCI DAA.
- Schedule and coordinate the testing of the release with Applications Lab personnel to allow developer participation in the Packaging and Certification process.

## **5.6 NMCI INTERFACES**

Interfaces to network infrastructure components are commonly identified by reading component specifications. Proper interfacing with enterprise infrastructures is required to ensure that the infrastructures continue to operate according to their original design and capacity.

This section identifies infrastructure interfaces, Application Program Interfaces (APIs), and specifications for the various types of applications that share the NMCI/IT-21 network environment. Developer responsibilities and common approaches to these interfaces are enumerated in an effort to protect, respect, and maximize the investment in the common enterprise network infrastructure. The goal for a developer should be to develop NMCI/IT-21/ MCTN applications that work securely and harmoniously with common network resources. Both NMCI and TFW participate in this object model through AD.

Information on Win32 API and the Microsoft Active Directory Service Interface (ADSI) model is available at <http://www.microsoft.com/windows/reskits/webresources>.

### **5.6.1 Windows 2000 Desktop Application Interface Specification**

Microsoft provides the Windows 2000 standard desktop specification at <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli.asp>.

This section describes the standard Windows 2000 APIs used in NMCI workstations and discusses NMCI use of Novadigm Radia (a software distribution system) and AD technologies that manage resource availability of both software and hardware, based on workstation or NMCI end user accounts.

Desktop applications developed for the NMCI Windows 2000 environment must undergo EDS certification processes, enumerated in Phase III, prior to deployment within the NMCI environment. The NMCI environment, monitored by EDS, protects connected user workstations, data, and application servers if and only if developers or users interfacing with the network need guidance. Applications and users are controlled as objects and removed from participation in NMCI if they violate policy or specifications.

### **5.6.2 Microsoft Windows 2000 Server Interface Specification**

Microsoft provides the Windows 2000 standard server specification at <http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2ksrv/html/w2kserve.asp>.

This specification provides resources to attain Windows 2000 certification (including checklists) and receive the MS Windows 2000 logo. Meeting the MS Windows 2000 logo specification produces a release that is NMCI compliant. However, a developer may encounter situations in which applications

must be developed which do not meet all MS Windows 2000 logo specifications. In cases where the GPOs, directory permissions, AD, firewall policy, and other settings cannot be met, the developer should contact the NMCI Help Desk for guidance.

### **5.6.3 Mobile Code**

Mobile code is a powerful software tool that enhances cross-platform capabilities, sharing resources, and web-based solutions. Its use is widespread and increasing in both commercial and Government applications. The DoD uses mobile code in systems to support FAs, ranging from acquisition to intelligence to transportation. Mobile code is not restricted from use within NMCI. However, when used, it must be fully compliant with established DoD standards. Mobile code, unfortunately, has the potential to severely degrade DoD operations if improperly used or controlled. More detailed information on mobile code is available at <http://iase.disa.mil/policy.html>.

## **5.7 BOUNDARY/NETWORK INTERFACE SPECIFICATIONS**

The type and strength of each security component is dependent upon the information protection requirements for a particular system. B1 reflects the Navy Marine Corps Enclave Protection Policy. B2 and B3 security mechanisms are flexible enough to meet the security requirements of various scenarios. Boundary configurations are tailored to provide the level of protection necessary to protect the integrity of NMCI and its users. NMCI also provides a wide-area IP backbone using DISA wide-area network (WAN) services with very high speed backbone network service (VBNS+) transport services. The Transport Boundary (TB) offers a secure encrypted intranet path between bases while imposing minimal restrictions on inter-base communications. Specific technical information on boundary requirements is available by contacting EDS IA personnel or the NMCI DAA.

Each system or application uses protocols to communicate between clients and servers. Many protocols and ports are associated with security vulnerabilities, and boundary policy reflects this. If an external application is compliant with B1 firewall policy, users within NMCI may access the application through the B1 boundary. To know if an application or system is compliant, its protocols, ports, and directions of activity must first be identified and characterized for assessment with respect to those of NMCI.

If an external system requires interaction not allowed by Navy/Marine Corps firewall policy, technical methods can obtain access through the boundary. The Navy/Marine Corps may choose to modify the baseline firewall policy to permit access to a system. Access may be possible through a virtual private network (VPN) path. A risk assessment must be prepared to determine whether a modification to firewall policy or the use of a VPN is acceptable. The NMCI DAA and local DAA use C&A documents to assess risks and make firewall policy modifications. A risk assessment does not need to be a one-at-a-time process; several applications can be considered simultaneously, if they run on shared servers and use the same ports/protocols.

### **5.7.1 Transport Boundary (TB)**

The TB is a suite of network security components configured to provide WAN network security.

### **5.7.2 Boundary 1 (B1)**

The B1 resides at the NOC and is designed to protect access to NMCI from the Nonsecure Internet Protocol Router Network (NIPRNET) and Secure Internet Protocol Router Network (SIPRNET). This boundary protects NMCI users and services located in external networks (i.e., IT-21, MCTN, and Defense



Information Systems Network - DISN). The B1 uses the Navy Marine Corps Enclave Protection Policy (NCEPP). The specifications for the B1 are available at <https://www.infosec.navy.mil>.

### **5.7.3 Boundary 2 (B2)**

The B2 resides at the site and is designed to interface NMCI with the site legacy network. The B2 allows application reach back into the legacy network. The B2 is a transitional boundary that will no longer be employed once all Navy and Marine Corps networks migrate to NMCI. The specifications for the B2 can be obtained from the NMCI DAA (NNWC and HQMC C4).

### **5.7.4 Boundary 3 (B3)**

The B3 is provided for use by COI operating within the NMCI network.

### **5.7.5 Boundary 4 (B4)**

The B4 is composed of those measures taken to ensure secure operations and communications at the workstation or desktop level. This is accomplished through four primary methods: GPO settings, virus protection, intrusion detection, and compliance management.

## **5.8 NETWORK-RELATED APIS OTHER THAN STANDARD WINDOWS 2000 ADSI**

MS ADSI may prove useful in realizing the enterprise benefits of AD. Further information is available at [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adsi/active\\_directory\\_service\\_interfaces\\_adsi.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adsi/active_directory_service_interfaces_adsi.asp).

## **5.9 NMCI LOCKDOWN POLICY**

NMCI lockdown policies disseminated through the AD, and enforced through GPOs, are highly restrictive settings that differ from the recommended MS Windows 2000 GPOs. Essentially, the application may write to its own area of a workstation disk with administrator privileges during install, but then must refrain from writing to restricted portions of the registry or other unauthorized areas of the disk at runtime.

## **5.10 SOFTWARE INSTALLATION**

For pushed or remote installations, the installation script is run as administrator, but the same lockdown policy applies at runtime. Applications deployed to NMCI clients should be placed in a folder under the directory C:\PROGRAM FILES.

## **5.11 SCREEN SAVER**

NMCI seats are set with the NMCI ISF screen saver. The screen saver activates after 15 minutes of inactivity and the user is prompted for a password to log back into the active desktop. The desktop user cannot change this.

## **5.12 TERMINAL SERVICE**

From a “terminal service” perspective, “NMCI Thin Client” architecture supports MS Windows 32-bit applications. The Citrix components (Nfuse, etc.) can interoperate with the NMCI portal. This enables the

launch of PC-based applications from the portal, display across the intranet, and the appearance of running locally while running remotely.

### **5.13 TESTING CONSIDERATIONS**

Applications must successfully complete the Developer Test and Evaluation (DT&E), including the creation of test scripts and test cases. The application must be verified to work on an NMCI-certified workstation. Developers must describe the types of tests done in the NMCI Certification process:

- Will the application print?
- Will MS Office applications continue to operate?
- What are the considerations for prototype/pilot testing?
- What are the steps, data, and logical conditions necessary to trigger programmed authentication processes (LDAP, AD, file sharing, file writes, etc.)?

This ensures that group policy, lockdown, and security areas are thoroughly examined by the Certification and DT&E. Developers must ensure that logon IDs have the same access rights as end users, not developers. For detailed instruction on the DT&E, contact the EDS Applications Lab.

## 6.0 NMCI RELEASE DEPLOYMENT PROCESS (NRDP)

Integration of a release within NMCI requires application developers to complete documentation, reviews, and tests. The NRDP is a formal process that defines the processes that a release must follow for packaging, testing, certification, and deployment in NMCI. This section describes the major process steps and basic considerations.

**NOTE:** For updated instructions on specific areas, be sure to check with the ISF Tools Database:  
<https://usplswebh0ab.plano.webhost.eds.net/isftool/Login.jsp>.

This section focuses on the introduction of new (emerging) releases into NMCI; the processing of quarantine/kiosk application solutions; and the deployment of patches, modifications, fixes, updates, and upgrades to existing applications operating in NMCI.

The NRDP, as depicted in Figure 6-1, is part of the overall management strategy of the NRMP. The process ensures that all releases are compliant with established standards, directs actions to be taken when compliance is not achieved, and covers steps involved in deployment of the release. Figure 6-2 is the legend for process flow diagrams used in this section.

All CNO guidance, Naval messages, and requirements addressed in the NRDDG apply in the processing of classified releases. The classified release process is very similar to that for unclassified releases. This section addresses the differences.

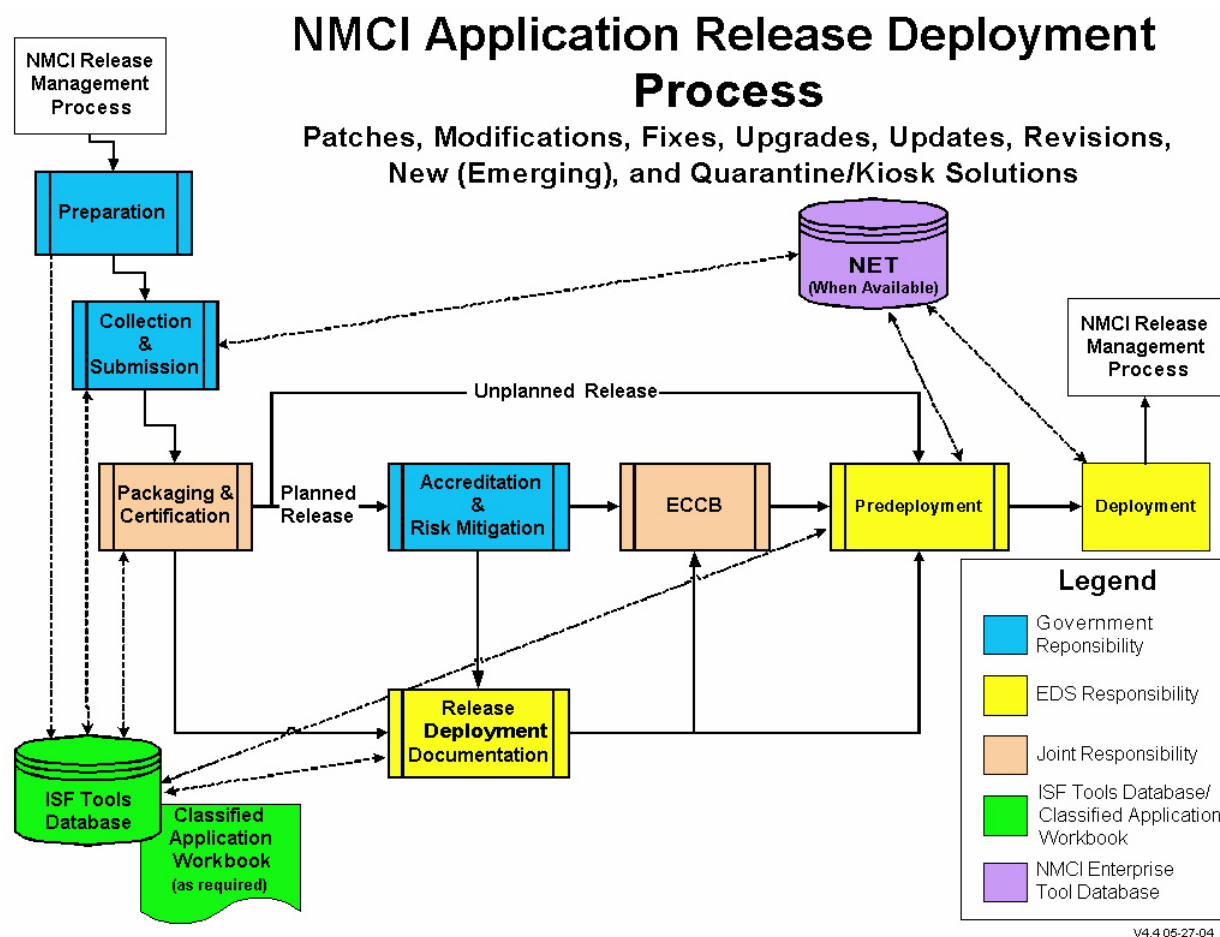
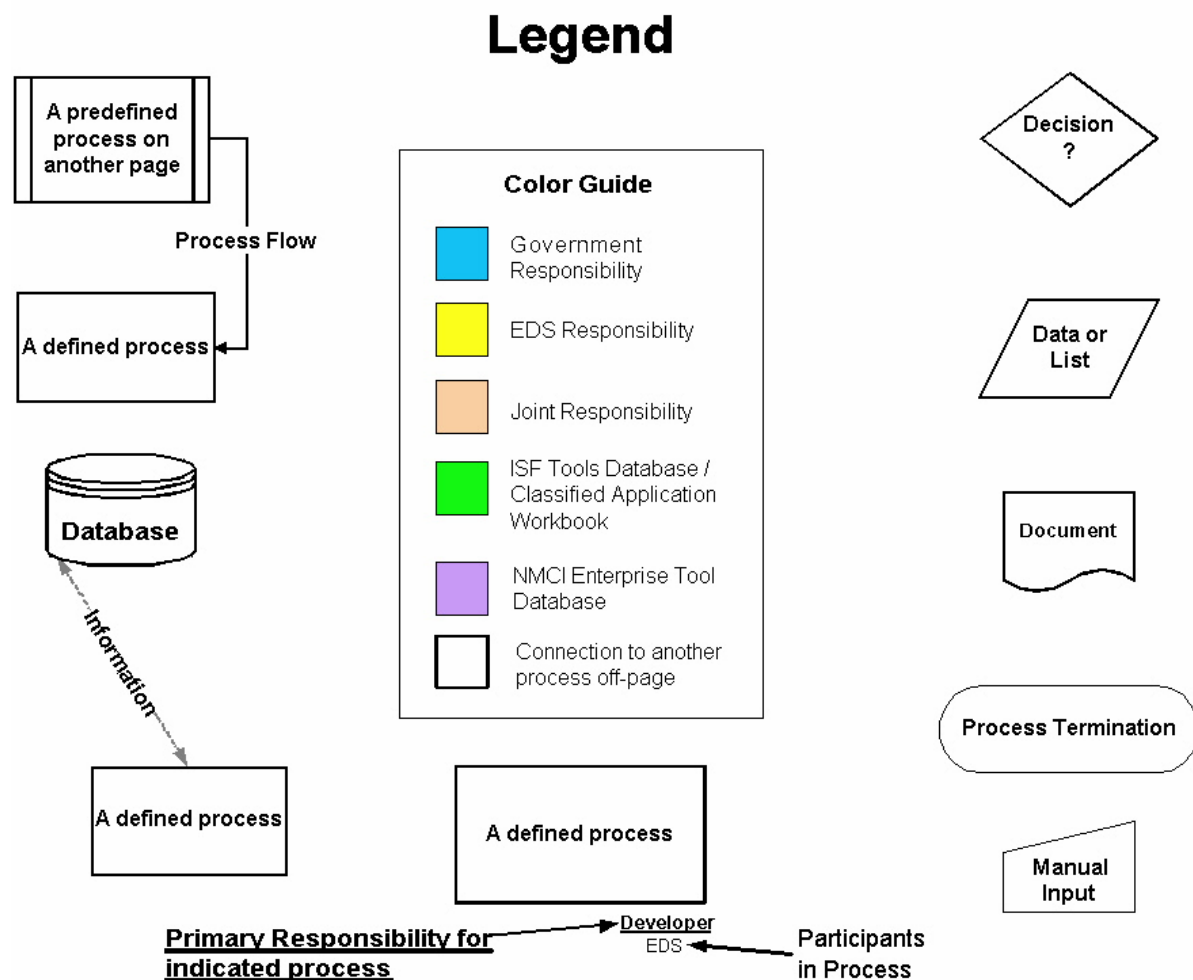


Figure 6-1 NRDP



V4.4 05-27-04

**Figure 6-2 NRDP Legend**

## 6.1 RELEASE DEPLOYMENT PLAN (RDP)

The RDP provides specific information pertaining to a release that supports its deployment. It contains all documentation used throughout the NRDP to allow informed decisions regarding the release. The developer is responsible for plan development and maintenance. The developer, EDS, and release sites use this plan to manage the successful deployment of the release. [Appendix G](#) provides a template for the RDP.

The plan documents all information pertaining to reengineering or fixes made to the release to satisfy testing and compliance requirements. If certain functions of the release are known not to work, they are documented in the plan.

Developers are encouraged to use existing documents as part of the plan and should only create or capture information that was not documented previously. The plan is submitted electronically on a CD.

## **6.2 REQUEST TO DEPLOY (RTD)**

The RTD process is the only authorized means for achieving release approval and deployment into NMCI. This subsection provides detailed explanations of the NMCI RTD and the Prioritization and Scheduling process for planned and unplanned releases.

NNWC is the designated approval authority for all Navy releases being submitted for deployment into NMCI. In executing this responsibility, NNWC has established an NRPM and an NRSN responsible for overseeing the NRMP.

HQMC(C4) is the designated approval authority and NRPM for all Marine Corps releases being submitted for deployment into NMCI. MCSC EBSS is the Marine Corps NRSN.

The NRPM and NRSN accept all submitted RTDs for planned releases that are ready for deployment. All unplanned releases are submitted on an as-required basis and are processed upon receipt.

Submit RTDs electronically to:

**Navy:** [nmci\\_scm@spawar.navy.mil](mailto:nmci_scm@spawar.navy.mil).

**Marine Corps:** [smbatnmci@mcsc.usmc.mil](mailto:smbatnmci@mcsc.usmc.mil).

[Appendix J](#) contains the RTD form and RTD Instruction Guide (RIG). An electronic version of the RTD is available at the NMCI sites: [www.nmci.navy.mil](http://www.nmci.navy.mil) and [www.nmciinfo.mcsc.usmc.mil](http://www.nmciinfo.mcsc.usmc.mil).

### **6.2.1 Quarantine/Kiosk Solutions [New (Emerging)]**

Once a quarantine/kiosk application has a remedial solution, that solution is introduced into NMCI through the NRDP, starting with the RTD. The solution is handled the same as any other release; e.g., patch, modification, fix, upgrade, update, revision, or new (emerging).

Once the quarantine/kiosk solution has been deployed through the NRDP, it is removed from the quarantine/kiosk desktop and the legacy network. If the quarantine/kiosk (dual) desktop is no longer needed, it is also removed.

### **6.2.2 Quarantine/Kiosk Solutions (Using an Existing Radia Application)**

Quarantine/kiosk applications that are remediated through the deployment of an existing NMCI application follow the RRPTE process, as discussed in Paragraph 3.5.6.6.

Once the quarantine/kiosk solution has been deployed through the NRDP, it is removed from the quarantine/kiosk desktop and the legacy network. If the quarantine/kiosk (dual) desktop is no longer needed, it is also removed.

### **6.2.3 Type of Release**

During the Preparation process, the developer must determine if the release is a planned annual or point release or an unplanned Emergency/Urgent release. The developer must provide sufficient justification for all Emergency/Urgent submissions to support the requirement for approving a higher-priority release over other releases into the NRDP.

### **6.2.3.1 Planned Release**

The planned release is the fundamental process for submitting planned periodic upgrades to existing applications, quarantine/kiosk solutions, and the introduction of new (emerging) applications operating in NMCI. This includes documentation, packaging, testing and certification, accreditation and risk mitigation, and deployment.

The two types of planned releases are 1) planned annual release and 2) planned point release.

A planned annual release is a major modification or upgrade and is part of an annual application release or refresh plan. No more than two annual releases may be submitted for the same application in any calendar year.

A planned point release is a minor change that is not considered part of the annual refresh plan and is based on business processes, security, or fiscal changes, etc. No more than four planned point releases may be submitted for the same application in any calendar year.

#### Annual Release Plan

- Based on business changes
- Planned at least one year ahead
- Is part of the annual technology refresh plan
- Includes versions and major releases
- Requires IATO/ATO
- Is limited to no more than two normal releases per year

#### Planned Point Release Plan

- Based on business and technical changes
- Planned six months ahead
- Is limited to no more than four releases per year
- Requires update to IATO/ATO
- Includes minor changes, patches, modifications, upgrades, and updates
- Includes quarantine/kiosk application solutions

### **6.2.3.2 Unplanned Release**

The unplanned release process supports the deployment of a release that requires expedited handling through the NRDP. This is to repair an application that is nonoperational or has significant technical problems that render it incapable of performing its intended function. Quarantine/kiosk solutions that fit into this category are also considered unplanned releases. Unplanned release deployment is handled identically to the planned release deployment, with the following exceptions:

- Emergency/Urgent releases may be submitted at any time.
- They must be justified and approved by NNWC/HCMC(C4).

#### Emergency/Urgent Release Plan

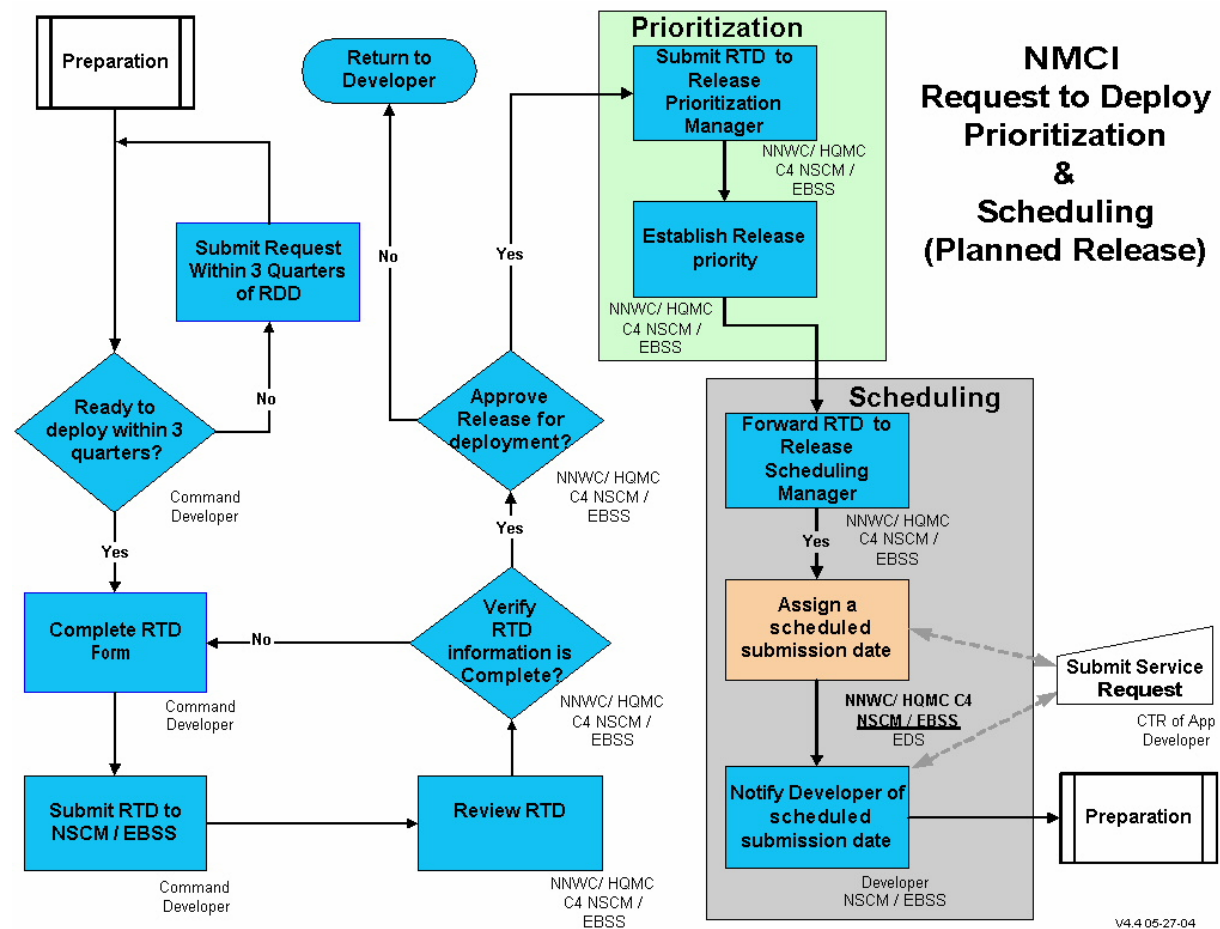
- Not planned, technical changes
- IA assessment to evaluate risk
- Minor changes, patches, modifications, or fixes
- Runs normal process with urgent priorities assigned in a shortened timeframe

## 6.3 RELEASE APPROVAL, PRIORITIZATION, AND SCHEDULING

The Release Approval, Prioritization, and Scheduling processes are designed to take a release through the formal steps at the beginning of the NRDP. The entire process begins with the RTD.

### 6.3.1 NMCI RTD Prioritization and Scheduling (Planned Release)

Figure 6-3 displays the steps that the developer must follow to obtain NNWC/HQMC(C4) approval to deploy a release and complete the Prioritization and Scheduling processes.



### Figure 6-3 NMCI RTD Prioritization and Scheduling (Planned Release)

### 6.3.1.1 Ready to Deploy Within Three Quarters?

First, determine if the proposed release can be deployed within the next three quarters.

Once development has been completed on an application, the NRDP is prepared, and the developer must determine whether the release can successfully be deployed into the NMCI environment within the next three quarters. If approved by the developer and Sponsoring Command, the RTD is initiated, and the Planned Release process continues. If the release cannot be deployed within the current timeframe, the developers retain the release until it is ready to deploy within the three-quarters requirement.



### **6.3.1.2 Complete RTD Form**

The RTD provides the basic information that NNWC/HQMC(C4)/EBSS uses to approve, prioritize, and schedule a release that supports an existing application, quarantine/kiosk solution, or a new (emerging) application being deployed in NMCI. The RTD form essentially drives the NRDP.

The developer and Sponsoring Command are responsible for completing the RTD. They are responsible for its validity and must ensure that it contains sufficient information regarding the release to enable NNWC/ HQMC(C4) to approve and establish prioritization. Although some information on the RTD has been noted to duplicate data contained on the CDA RFS/USMC RFS and DADMS questionnaire, the information on all forms is necessary to ensure releases are processed in an efficient and systematic manner. As the process becomes further refined, the vision is to transition the RTD into an online automated format that can capture reusable data from other sources to prepopulate the form and streamline the Submission process.

### **6.3.1.3 Submit RTD to NSCM/EBSS**

The Sponsoring Command reviews and approves the completed RTD prior to submission to NNWC/HQMC(C4)/EBSS for review and approval.

Submit RTDs electronically to the following email addresses:

**Navy:** [nmci\\_scm@spawar.navy.mil](mailto:nmci_scm@spawar.navy.mil).

**Marine Corps:** [smbatnmci@mcsc.usmc.mil](mailto:smbatnmci@mcsc.usmc.mil)

### **6.3.1.4 Review RTD**

NNWC has overall responsibility for ensuring that Navy applications destined for NMCI meet all approved and established conformance requirements. ([Section 4.0](#) and [Section 5.0](#) detail these requirements.) EBSS has RTD review responsibility for the Marine Corps. As a result, the RTD should be thoroughly reviewed to ensure that it is complete and contains the necessary information needed to process the request.

### **6.3.1.5 Verify Release Information Is Complete**

RTDs are most commonly rejected due to incomplete, missing, or erroneous data, or because the NRPM needs the input to be clarified. RTDs that are incomplete or found to be outside the established submission criteria are returned to the developer for corrective action or are held for submission at a later date. Once corrected, the RTD is resubmitted and the process continues.

### **6.3.1.6 Approve Release for Deployment**

Before a developer can begin the deployment cycle, the developer must receive authorization to deploy the release in NMCI. Based on the review and acceptance of the RTD, NNWC/HQMC(C4) approves or disapproves the application for deployment. When the information on the RTD has been verified as complete and accurate, the NRPM decides whether to approve the deployment. If the request is denied, the developer and Sponsoring Command are notified of the disapproval and given a detailed description of the disapproval reason, and the RTD is returned without action. If the request is approved, the RTD proceeds to prioritization.

### **6.3.1.7 Submit RTD to Release Prioritization Manager**

Normally, approved RTDs are prioritized using the “First In, First Out” (FIFO) method. If additional prioritization is warranted, the NNWC/HQMC(C4) NRPM processes the release to determine its priority.

### **6.3.1.8 Establish Release Priority**

A systematic scoring method has been developed to determine the priority of a release for scheduling. When a release enters the Prioritization process, it is assigned a weighted score based on information provided on the RTD. When the score has been assessed, a priority is assigned and the RTD is then passed to the NRSRM for scheduling.

### **6.3.1.9 Forward RTD to Release Scheduling Manager**

Once prioritization is complete, the RTD is forwarded to the NNWC/MCSC EBSS NRSRM, who assigns it a scheduled submission date.

### **6.3.1.10 Assign a Scheduled Submission Date**

In determining a scheduled submission date, the NRSRM reviews the weighted score, complexity, required deployment date, and the date the release will be ready for submission to the Applications Lab. The NRSRM adjusts the overall schedule to accommodate any priority applications.

### **6.3.1.11 Notify Developer of Scheduled Submission Date**

Once a submission date to the Applications Lab has been established, the NRSRM notifies the developer. The developer must ensure all requirements have been met for submission of a release to the Applications Lab on the scheduled submission date. Paragraph 6.6 contains requirements for application submission.

## **6.3.2 NMCI RTD Prioritization and Scheduling (Unplanned Release)**

The unplanned release process supports the deployment of a release that requires expedited handling through the NRDP to repair an application that is nonoperational or has significant technical problems that render it incapable of performing its intended function.

The unplanned release process is identical to the planned release process with the following exceptions:

- Emergency/Urgent releases may be submitted at any time.
- They must be justified and approved by NNWC/ HQMC(C4).

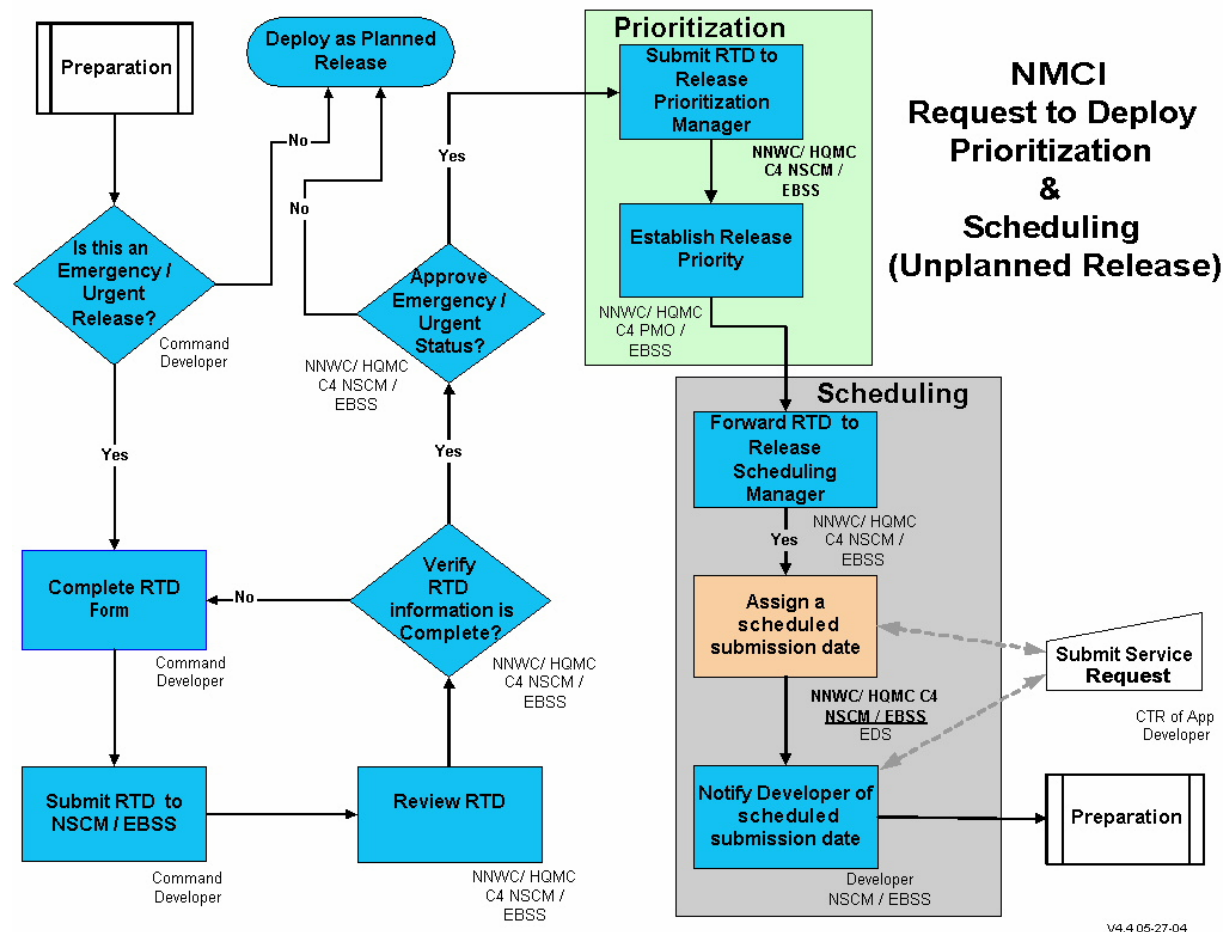
The RTD is marked as an unplanned Emergency/Urgent release. It is submitted and processed on an as-required basis to support mission-essential applications. Special care must be given to justify the requested status in order to ensure that necessary information is provided to enable NNWC/ HQMC(C4) to determine a rapid approval.

Figure 6-4 displays the steps the developer and Sponsoring Command must follow to obtain NNWC/ HQMC(C4) approval to deploy an unplanned Emergency/Urgent release and complete the Prioritization and Scheduling processes. The following paragraphs address only those areas that differ from the Planned Release process.

RTDs must be submitted electronically for processing to the following email addresses:

**Navy:** [nmci\\_scm@spawar.navy.mil](mailto:nmci_scm@spawar.navy.mil).

**Marine Corps:** [smbatnmci@mcsc.usmc.mil](mailto:smbatnmci@mcsc.usmc.mil)



**Figure 6-4 NMCI RTD Prioritization and Scheduling (Unplanned Release)**

### 6.3.2.1 Is This an Emergency/Urgent Release?

The developer and Sponsoring Command must determine if the release has an Emergency/Urgent requirement. NNWC/HQMC(C4) considers all unplanned Emergency/ Urgent releases on an as-required basis upon submission. Developers must ensure that clear and concise information is provided that justifies the requirement for an Emergency/Urgent release. All unplanned release submissions are processed within three working days of receipt.

### 6.3.2.2 Approve Emergency/Urgent Status

NNWC/HQMC (C4) review pays special attention to the justification and may request additional information or clarification prior to making a determination. When the information on the RTD has been verified as complete and accurate, NNWC/HQMC(C4) approves or disapproves the request for an unplanned (Emergency/Urgent) release deployment. If the request is disapproved, the developer is

notified and the RTD is prioritized and scheduled as a planned release. Appeals on the disapproval can be made directly to NNWC/HQMC(C4). An approved request is submitted for prioritization as an unplanned (Emergency/Urgent) release.

### **6.3.2.3 Assign a Scheduled Submission Date**

Based on priority established by the NRPM, release media availability date, and required deployment date, the NRSM schedules the Emergency/Urgent release to ensure the earliest opportunity to deploy.

### **6.3.3 RTD Cancellation Process**

The developer is responsible for ensuring that all required deliverables are submitted on time to EDS. Failure to comply with established milestones creates significant release deployment delays, unnecessarily tying up limited resources that can be employed supporting other mission-critical application releases.

The NMCI PMO, in conjunction with NNWC, established a policy for the cancellation and resubmission of RTD-sponsored applications. The cancellation policy applies to developers who fail to meet required Government milestones. Developers are responsible for providing complete and accurate applications submission packages consistent with the NRDDG.

The failure of a developer to supply complete and accurate information in a timely manner at the following key milestones cancels the RTD:

- Media submission date negotiated between the NSCM and developer
- Issuance of the certification letter after media submission. (This is 20 days for a nonplanned release or 45 days for a planned release.)
- Submission of a complete RDP and pilot-test mapping.

This cancellation and resubmission policy is required to ensure resources focus on post transition applications that have completed documentation, as defined in the NRDDG. This policy applies only to applications submitted for test, certification, and deployment to NMCI seats through the required process. Sponsored applications are cancelled if the developer fails to comply with the submission of required documentation, media, or other Government furnished information (GFI).

The NMCI Software Configuration Management (NSCM) office sends a compliance notice to the developer through telephone and e-mail when an application misses an RTD major deliverable date (media, RDP, etc.). The compliance notice states that the developer has 48 hours to submit the nonplanned RTD deliverable or 2 weeks to submit the planned deliverable. If the developer does not meet the compliance notice requirements, that application RTD is referred to the NNWC (Navy) or the MCNOSC (Marine Corps) for cancellation and rescheduling. Upon confirmation of cancellation from the NNWC or MCNOSC, the NSCM notifies the developer and its command that the RTD has been cancelled and the RTD for the application must be resubmitted. The cancellation notice provides the following information:

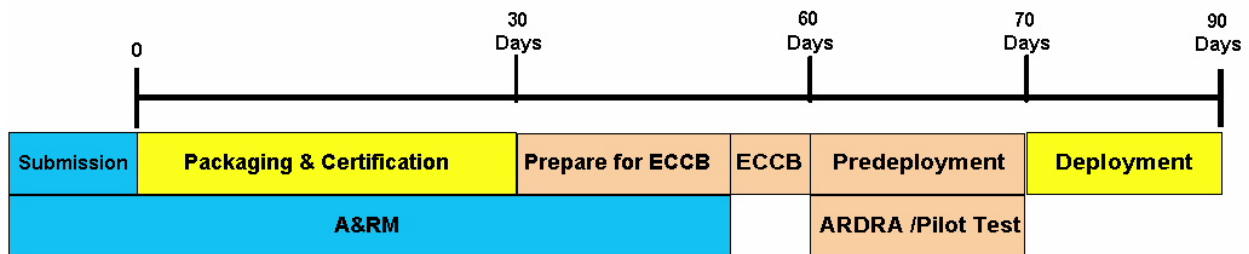
- Guidance for resubmission of a new RTD
- Identification of the NSCM CCS POC to assist the developer with resubmission.

## 6.4 TIMELINE FOR NRDP

### 6.4.1 Notional Processing Timeline for Planned Releases

In order to maintain control and discipline in the NMCI environment, a formal Submission and Deployment process is followed. Figure 6-5 depicts the notional timeline for submitting and processing a planned release. This timeline is meant as a guideline. A release may complete the process in less but no more than the 90 calendar days indicated. The NRDP follows the pattern from left to right.

#### NMCI Notional Application Release Deployment Process Timeline (Planned Release)



#### Annual Application Release Deployment Plan

- Planned Business Changes
- Part of the Annual Technology Refresh Plan
- Full Accreditation Required – DITSCAP
- No more than 2 normal releases per year
- Plan at least one year ahead
- Versions & major releases
- Calendar Days

#### Planned Point Release Plan

- Business Changes, Technical Changes
- Done quarterly with no more than 4 per year
- Minor changes, patches, modifications, upgrades, updates
- Plan with six-month notice
- Update to IATO/ATO required
- Calendar Days

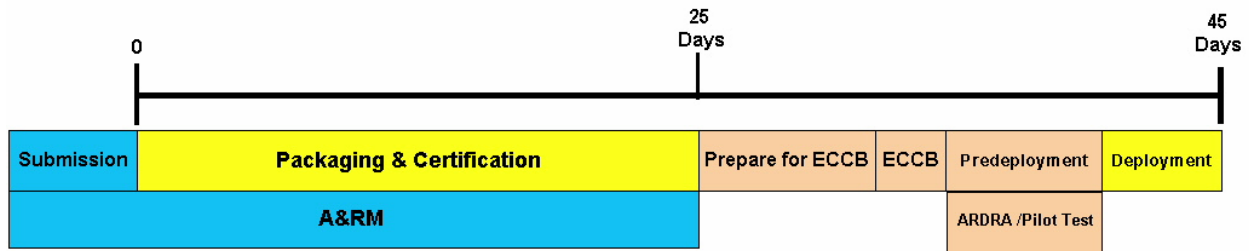
V4.4 05-27-04

**Figure 6-5 Timeline for NMCI Application Release Deployment Process (Planned Release)**

### 6.4.2 Notional Processing Timeline for Unplanned Releases

Figure 6-6 depicts the notional timeline for submitting and processing an unplanned release. This timeline is meant as a guideline. A release may complete the process in less but no more than the 45 calendar days indicated. The NRDP follows the pattern from left to right.

## NMCI Notional Application Release Deployment Process Timeline (Unplanned Release)



### Emergency / Urgent Release Plan

- Not Planned, Technical Changes
- Minor changes, patches, modifications, fixes
- Runs normal process with urgent priorities assigned in a shortened timeline from a Planned Release
- IA Assessment to evaluate risk
- Calendar Days

V4.4 05-27-04

**Figure 6-6 Timeline for NMCI Application Release Deployment Process  
 (Unplanned Release)**

### 6.4.3 Submission

To avoid overwhelming the system, the developers have an assigned specific submission date to deliver their releases to the Applications Lab for processing. The developer is responsible for ensuring that the release has completed development prior to scheduled submission date. In the event a scheduled submission cannot be met, the developer would notify the designated CCS representative assigned the release to remove that release from the schedule. Once the situation that caused the release to be removed from the submission schedule is resolved, the developer asks the designated CCS representative to assign a revised submission date.

### 6.4.4 Receipt, Audit, Packaging, and Certification

The next segment of the timeline is the Release Deployment Process is the Receipt, Packaging, and Certification processes. The EDS processes the release at the Applications Lab in San Diego. The application is received, audited, packaged, client tested, connectivity tested (if required), and certified, with status maintained in the ISF Tools Database. The developer is required to participate in this testing. Although this segment is notionally depicted as 45 calendar days, it could be much less.

#### **6.4.5 Accreditation and Risk Mitigation (A&RM)**

A&RM is required for annual releases and those releases that have an impact on the IA posture of an application. The supporting documentation for the A&RM process actually starts the moment a release is conceived. This 10-day period includes the finalizing and submission of the A&RM (DITSCAP) documentation to the NMCI PMO/MCNOSC for review and submission to the NMCI DAA/USMC DAA.

#### **6.4.6 Enterprise Change Control Board (ECCB)**

The final release solution and IA impacts for a release are submitted for review and approval by the ECCB. A formal ECCB output and approval is required for all annual releases and those point or unplanned Emergency/Urgent releases that have an IA impact.

#### **6.4.7 Application Release Deployment Readiness Activity (ARDRA)**

ARDRA is a process that actually starts once the packaging, certification, and testing in the Applications Lab and San Diego NOC labs are complete. These 20 calendar days are used to address any testing needed to ensure a successful deployment at the sites/bases involved. ARDRA is conducted on-site and is not a mandatory step, but is used when a specific deployment concern needs addressing at the site. The decision to pretest the release for deployment rests jointly with the specific EDS SM and the developer.

#### **6.4.8 Release Push/Deployment to the Desktop**

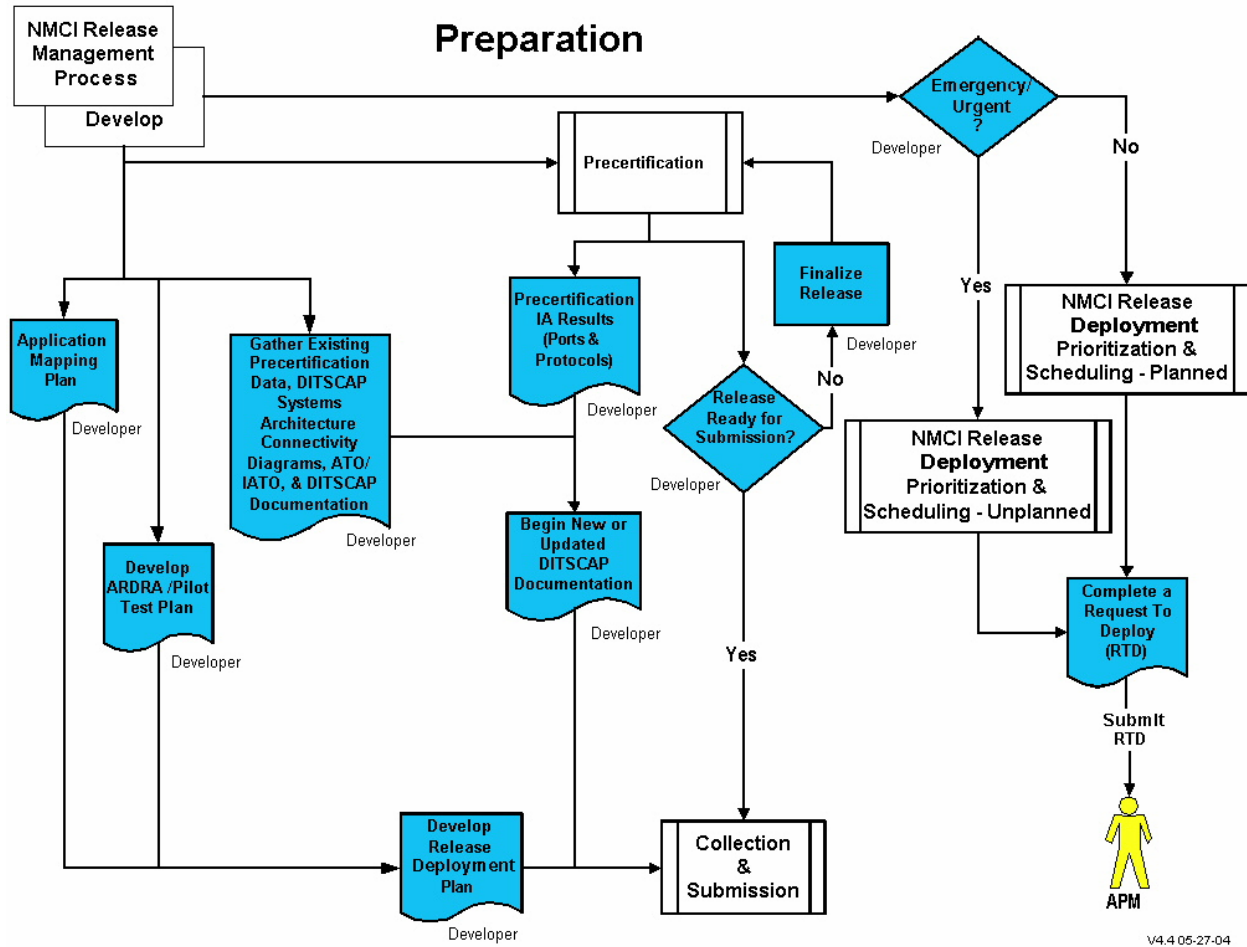
Once the release has completed all testing and received all approvals, it is pushed or locally loaded to the desktop. EDS SMs and developers play an important role in these steps.

### **6.5 PREPARATION**

Figure 6-7 depicts the Preparation process through which the developer begins to collect, document, and organize information prior to submission of the release for packaging, testing, certification, and deployment. During this process, the developer completes the following tasks:

- Begin Application Mapping Plan
- Develop ARDRA/Pilot Test Plan
- Gather Existing Precertification Data, Systems Architecture Connectivity Diagrams, ATO/IATO, & DITSCAP Documentation
- Precertification
- Begin New or Updated DITSCAP Documentation
- Develop RDP





**Figure 6-7 Preparation Process**

### 6.5.1 Begin Application Mapping Plan

The developer must work closely with the sites to ensure that application mapping is performed to the support the deployment of the release. EDS uses this information to ensure that the release is deployed in accordance with the application mapping document contained in the RDP (see [Appendix I.3](#)).

### 6.5.2 Develop ARDRA/Pilot Test Plan

The key to the success of the ARDRA/Pilot Test is a well designed plan. This requires commitment from appropriate Commands, planning for availability of personnel and equipment, but most importantly, communications between all parties, including EDS, developer, affected customers, and Commands. As part of the RDP, the developer must develop an ARDRA/Pilot Test plan well in advance of the start of the test. (Refer to the ARDRA/Pilot Test checklist in [Appendix I.6](#).)

### 6.5.3 Gather Existing Precertification Data, Systems Architecture Connectivity Diagrams, ATO/IATO, & DITSCAP Documentation

At this point in Preparation, the developer has gathered all existing C&A information, such as Systems Architecture Connectivity Diagrams, existing ATO/IATO, DITSCAP documentation, DITSCAP, and any



other pertinent documentation, for use in obtaining a final ATO from the NMCI DAA. This information is kept on file with the developer for use later in the process as the final DITSCAP documentation is developed and submitted.

Development and update of System Architecture Connectivity Diagrams are used to define the desktop and server connection topology as part of the DITSCAP process. This topology must also include the ports and protocols required for the desktop to communicate across the boundary to the hosting services. The System Architecture Connectivity Diagrams become part of the DITSCAP documentation.

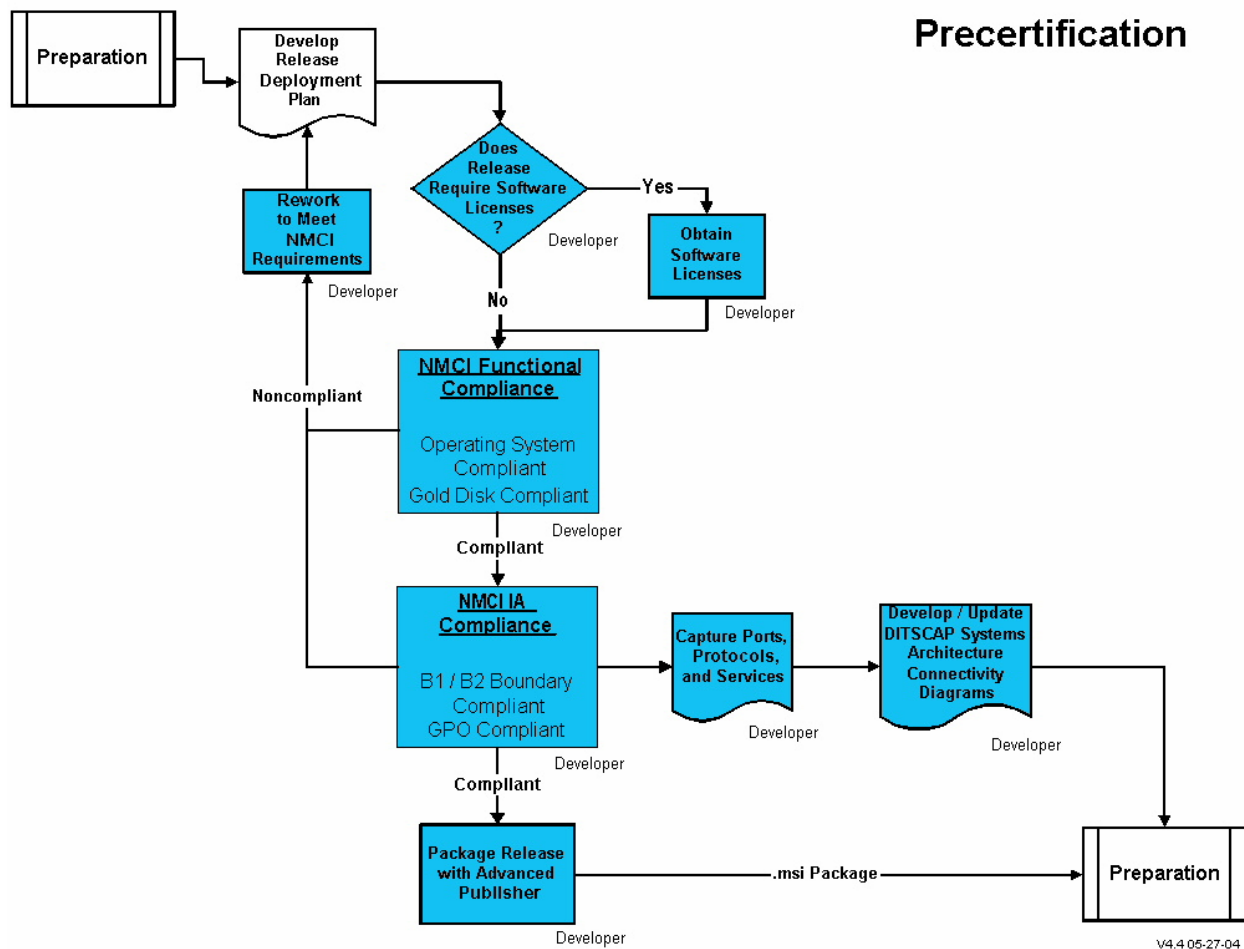
Inventory and cataloging of all data pertaining to Precertification and the ATO/IATO must be performed during Preparation. This information is entered into the RDP and is used throughout the Release Deployment Process.

#### **6.5.4 Precertification**

Figure 6-8 depicts the Precertification process, which is designed to evaluate the release to ensure its compliance with the NMCI software configuration and operating environment standards. Performance of Precertification ensures that the submitted release meets those standards; this eliminates the potential for the EDS Applications Lab becoming a developer Beta test site. For the Navy, the NMCI PMO performs Precertification for all applications with the developer at the NMCI PMO Precertification facility in San Diego, CA. Navy application developers must submit their Application Submission Packet to the NMCI PMO Precertification facility in San Diego, CA. For the Marine Corps, EBSS performs Precertification centrally with the developer at the Marine Corps Applications Integration Testing Laboratory (MCAIT Lab) in Quantico, VA. During this process, the developer completes the following tasks:

- Obtain software licenses.
- NMCI functional compliance
- NMCI IA compliance
- Capture ports, protocols, and services
- Develop/update systems architecture connectivity diagrams.
- Release package with Advanced Publisher

For classified applications the ports, protocols, and services information is protected and is documented in the Classified Application Workbook.



**Figure 6-8 Precertification Process**

#### 6.5.4.1 Obtain Software Licenses and/or License Keys

All applications that operate in NMCI must have the appropriate licenses and/or license keys. Software licenses are commonly obtained with the software purchase or can be purchased separately for additional users. The license explains the terms and agreements for use of the subject software. Developers must submit a copy of the software license.

Navy policy requires that all software operating on an NMCI seat have a valid license, if required. The Government is responsible for ensuring that this requirement is met. The Application Submission Packet includes a copy of the license, if required,

#### 6.5.4.2 NMCI Functional Compliance

This task ensures that the release is compliant with the operating system and the Gold Disk load set.

### **6.5.4.3 NMCI IA Compliance**

This task ensures that the release is compliant with the NMCI enclave protection policy (Boundary 1), the legacy-to-NMCI network connectivity (Boundary 2), and Group Policy Object (GPO) (Boundary 4) security requirements.

### **6.5.4.4 Capture Ports, Protocols, and Services**

This task documents the ports, protocols, and services used by the release to satisfy connectivity requirements beyond the desktop. This information is used as part of the development of the new or updated DITSCAP documentation and as part of a Boundary Change Request, if required.

### **6.5.4.5 Develop/Update Systems Architecture Connectivity Diagrams (DITSCAP)**

This task requires the development and update of System Architecture Connectivity Diagrams to define the desktop and server connection topology as part of the DITSCAP process. This topology must also include the ports and protocols required for the desktop to communicate across the boundary to the hosting services. The System Architecture Connectivity Diagrams become part of the DITSCAP documentation.

### **6.5.4.6 Package Release with Advanced Publisher**

For NMCI certification testing, EDS accepts either raw media or Microsoft installer-compliant installation packages (.msi) generated from Radia Advanced Publisher using the NMCI packaging standards. Refer to [Appendix K](#) for NMCI packaging standards/best practices for MSI.

Currently, the EDS agreement with Novadigm is to allow only ‘.msi’ packages created with Radia Advanced Publisher to be used within NMCI. Novadigm is allowing the use of Radia Advanced Publisher for NMCI application packaging at no additional cost.

Radia Advanced Publisher is a standalone software tool used to create ‘.msi’ packages. The goal of using Advanced Publisher is to create a compact, fully functional packaged application for deployment across the enterprise. NMCI has standardized Advanced Publisher as the tool of choice to create ‘.msi’ packages outside the Applications Lab. Radia Advanced Publisher is a field deployable version of the NMCI enterprise-wide software management tool called Novadigm Radia. EDS may deploy using either ‘.msi’ packaged applications or by converting them to Novadigm Radia packaged ‘instances’. (The latter is the long-term NMCI management strategy.)

NMCI uses Novadigm Radia to automate the management of software throughout the full deployment lifecycle to package, analyze, inventory, deploy, repair, update, and remove an application.

### **Use of Radia Advanced Publisher**

Radia Advanced Publisher does not require connectivity to a Radia server. It is wizard driven, which allows the developer/MCAIT Lab to make a standard (enterprise) configuration package (which should be the developer goal) from their own installed application. Specially configured packages that may be needed due to local or environmental requirements can also be created.

### **Required Training**

Radia Advanced Publisher training is available from EDS at its San Diego facility at no charge to developers at this time, but attendees must pay their own travel and lodging expenses. Radia Advanced

Publisher '.msi' received from developers that have not had at least one person attend EDS training are rejected. And '.msi' packages received from developers do not conform to NMCI packaging standards are rejected. MCAIT Lab personnel have attended EDS training in order to properly package Marine Corps applications.

EDS provides no more than one free copy of Radia Advanced Publisher to any developer that had at least one certified attendee in a Radia Advanced Publisher training class. Each class is 5 days long with no more than six people per class. If the class is conducted off-site, the requesting activity covers the instructor's travel and lodging expenses. Attendees of classes conducted in the San Diego EDS facility need to submit a Visit Authorization Letter (VAL) to the EDS Security Manager prior to the class. [Appendix I.5](#) provides more information on obtaining an EDS visit request.

This class has one terminal objective: Train developers to use the Radia Advanced Publisher to package .msi and non-.msi applications to NMCI packaging standards.

- Event 1: Packaging .msi applications. If developers have simple .msi applications that need packaging, attendees should bring them.
- Event 2: Packaging non-.msi applications. If developers have simple non-.msi applications that need packaging, attendees should bring them.
- Event 3: Packaging applications that have no installer. This event should be short and simple to allow the attendees ample opportunity to continue packaging their .msi and non-.msi applications.
- Events 4 and 5: The remainder of the week is spent packaging the two example applications used in class until the attendees get a feel for packaging each type of application. After that, the instructor works individually with the attendees on their own applications. Attendees attempt to package their own applications, and the class instructor performs quality assurance on their work. This way, attendees are trained and work on their applications.

For more information and the schedule for Radia Advanced Publisher classes, please contact Gary Smith at [gary.smith-eds@eds.com](mailto:gary.smith-eds@eds.com).

### **6.5.5 Begin New or Updated DITSCAP Documentation**

New or updated DITSCAP documentation must be submitted in accordance with the provisions of Paragraph 4.7 for all planned releases. The developer uses the information previously obtained by gathering existing IATO/ATO and DITSCAP documentation in order to complete this requirement.

The information contained in the DITSCAP documentation is used to obtain full accreditation and issuance of an IATO/ATO. The developer must determine whether the release requires a new or updated DITSCAP submission. Once these requirements have been met, the developer can submit the DITSCAP document to the service NMCI DAA for review and approval.

### **6.5.6 Develop RDP**

The developer begins creating the RDP as the last step of the Preparation process. The information obtained during the Preparation and Precertification processes forms the baseline for the RDP. The RDP is used throughout the Release Deployment Process, and the ECCB reviews it prior to deployment of the release. [Appendix G](#) contains an RDP template and user guide.

## 6.6 COLLECTION AND SUBMISSION

Figure 6-9 depicts the Collection and Submission process. This process results in the completion of an Application Submission Packet, an updated RDP and new/updated DITSCAP documentation. The Certification CLIN and SRM (MAC) or Distribution CLIN are submitted to the Service Request Team. NET will perform this submittal when it is available to support this requirement. During this process, the developer completes the following tasks:

- Generate a CDA RFS.
- Complete and submit an Application Submission Packet.
- Finalize and submit new or updated DITSCAP documentation.
- Update and submit the RDP.
- Submit Certification CLIN and SRM (MAC) or Distribution CLIN to Service Request Team.

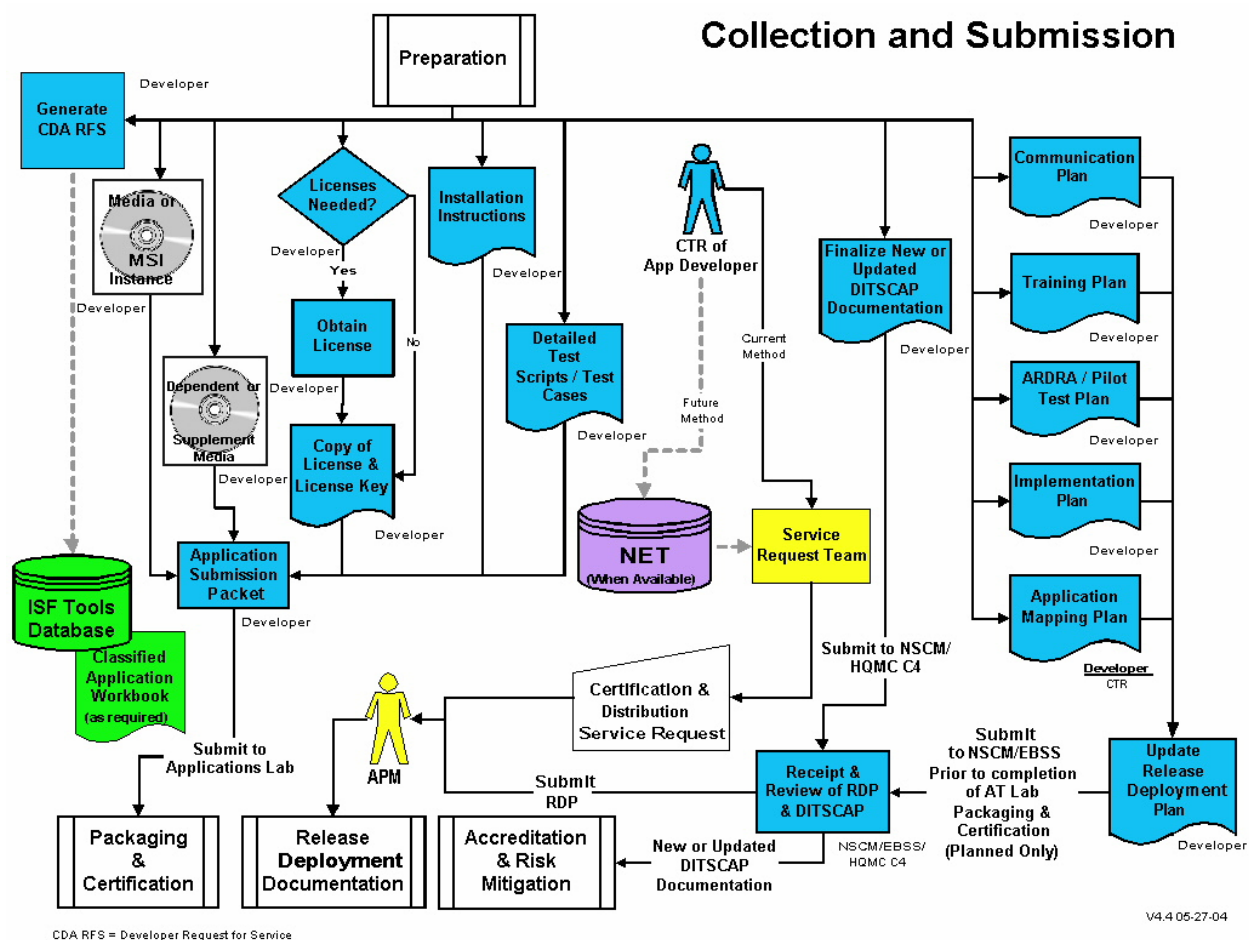


Figure 6-9 Collection and Submission Process

### 6.6.1 Generate CDA Request for Services (RFS)/USMC RFS

The Navy developer must complete a CDA RFS in the ISF Tools Database before the Application Submission Packet can be submitted to the Applications Lab or North Island NOC for processing. Marine Corps developers send an electronic RFS to EBSS ([smbatnmci@mcsc.usmc.mil](mailto:smbatnmci@mcsc.usmc.mil)) for input to the ISF

Tools Database. This RFS number is used to obtain information regarding the status of the release as it undergoes the NRDP.

The developer is responsible for maintaining information on all classified releases in the Classified Application Workbook and ISF Tools Database. Ports, protocols, services and IP addresses will be maintained in the Classified Application Workbook. Only personnel with appropriate security clearances may handle and store classified material

### **6.6.2 Application Submission Packet**

The developer creates an Application Submission Packet that consists of software media and documentation. Navy developers deliver their Application Submission Packet to the NMCI PMO Precertification facility in San Diego, CA for testing, certification, and deployment. Marine Corps developers deliver their Application Submission Packet to the MCAIT Lab for Precertification. The NMCI Precertification Lab and the MCAIT Lab then deliver the precertified packet to the EDS Applications Lab. The preferred method is to write the packet to a CD and ship it through a traceable means (e.g., FedEx, UPS, or registered mail). The developer is encouraged to retain a copy of the packet in the event of loss in transit. The Application Submission Packet contains the following:

- Media or .msi instance
- Dependant or supplemental media
- Copy of licenses and/or license keys
- Installation instructions
- Detailed test scripts/test cases

An Application Submission Packet is considered complete when the following requirements are met:

- RFS has been submitted in ISF Tools.
- A complete copy of the raw media or .msi instance is provided.
- Licenses and/or license keys are provided.
- Installation instructions are included.
- The software media is virus free.

If these conditions are not met, the Application Submission Packet is rejected. The deployment schedule will be adjusted once the new Application Submission Packet is received.

#### **6.6.2.1 Media or .msi Instance**

The EDS Applications Lab accepts either raw media or a Radia Advance Publisher .msi instance. This media consists of a clean and virus-free copy of the software. Only developers who received training and software from EDS to use Radia Advance Publisher may submit an .msi instance. Paragraph 6.5.4.6 provides more information on Advance Publisher training.

#### **6.6.2.2 Dependent or Supplemental Media**

If the release requires the use of dependent or supplemental software, as indicated in the RDP, a clean and virus-free copy of the software must be submitted with the Application Submission Packet. If the software was previously introduced into NMCI, the developer may request the Applications Lab to use the software version maintained in the DSL.

### **6.6.2.3 Copy of Software License and/or License Keys**

Navy policy requires that all COTS software and GOTS with embedded COTS software operating on an NMCI seat have a valid license. The Government is responsible for ensuring that this requirement is met. A copy of the license and/or license keys must be included in the packet,

### **6.6.2.4 Installation Instructions**

The Applications Lab uses the installation instructions as part of the Packaging process in creating a Novdigm Radia instance. The developer must ensure that the installation instructions document all specific tasks for a release to be properly installed on the NMCI seat. [Appendix I.2](#) provides an example of the installation instructions.

### **6.6.2.5 Detailed Test Scripts/Test Cases**

The detailed test scripts and test cases describe the objectives, scope, approach, and focus of the software test that are performed as part of Packaging & Certification by the Applications Lab. The detailed test scripts and test cases include the following:

- What items will be tested
- At what level will testing be performed
- What is the test sequence?
- How will the test strategy be applied to each item?
- What is the configuration of the test environment?

Each test plan is intended to verify and validate the software being tested. The software must satisfy its functional and operational design requirements.

A test case should contain the following items to determine that an application is functioning correctly:

- Test case identifier
- Test case name
- Objective
- Test conditions/setup
- Input data requirements.

Cases should be prepared early in the development cycle since thinking through the operation of the application can identify problems.

## **6.6.3 Update Release Deployment Plan**

Upon completion of all collection and submission tasks, the developer updates the RDP and forwards a copy of the completed RDP to the NMCI PMO for review and submission to the APM. During this process, the developer completes the following tasks:

- Develop Communications and Key Correspondence Plan.
- Complete Training Plan.
- Complete Implementation Plan.
- Complete ARDRA/Pilot Test Plan.

### **6.6.3.1 Develop Communications and Key Correspondence Plan**

A sound and effective communications plan is essential to the deployment of a release on the NRDP desktop. The plan includes any POCs (e.g., Government, EDS, and contractor support personnel) that the developer indicates require notification during the NRDP. This plan also includes key correspondence that supports the deployment of the release. The RDP documents and maintains this information.

### **6.6.3.2 Complete Training Plan**

The developer determines if the deployment of the release requires end user training. If training is required, the developer must provide a detailed description of that training and its anticipated completion date. The RDP includes this information.

If training is required for the implementation team, the developer must provide a Training Plan summary, and if necessary, attach a copy of the POA&M to the RDP.

### **6.6.3.3 Complete Implementation Plan**

The RDP contains information specific to the Implementation Plan. The developer must complete all questions on the RDP with regard to implementation.

### **6.6.3.4 Complete ARDRA/Pilot Test Plan**

The key to the success of the ARDRA/Pilot Test is a well designed plan. This requires commitment from appropriate Commands, planning for availability of personnel and equipment, but most importantly, communications between all parties, including EDS, developer, affected customers, and Commands. As part of the RDP, the developer must develop an ARDRA/Pilot Test plan well in advance of the start of the test. (Refer to the ARDRA/Pilot Test checklist in [Appendix I.6.](#))

### **6.6.3.5 Application Mapping Plan**

The Application Mapping Plan is critical to the successful deployment of applications to existing NMCI seats. Application mapping is a Government responsibility, but when possible, the Navy NMCI PMO NSCM Office (QUEST and CCS) and Marine Corps MCSC EBSS work with EDS to supply current mapping information for the application being upgraded or replaced. The developer must provide EDS with a complete Application Mapping Plan for release deployment. Refer to [Appendix I.3.](#)

For classified applications, the developer will identify the sites, servers, and users that will receive the release. Developers must ensure that the documentation remains unclassified by omitting any ports, protocols, services, and IP addresses. EDS will use this information to ensure that the release is deployed to the proper sites, servers, and users.

The Application Mapping process begins upon release of a Naval message generated by the Navy NMCI PMO NSCM Office (QUEST and CSS). This message informs all activities about the progress of enterprise applications through the Deployment process. Upon receipt of the message, the developers and activities list all sites affected by the release and provide a complete application mapping for release deployment. The developer and activity or Command must announce the release to allow all subordinate users to coordinate with the site CTR/ACTR to ensure they are mapped to the release prior to deployment. EDS uses this information to ensure that the release is deployed in accordance with the application mapping.



The developer/CTR identifies and approves the application mapping of each release before EDS initiates deployment. Direct any questions or concerns on this subject to:

**Navy:** NSCM Service Desk at [NSCM\\_SCM@spawar.navy.mil](mailto:NSCM_SCM@spawar.navy.mil) or (619) 524-4554

**Marine Corps:** MCSC EBSS at [smbatnmci@mcsc.usmc.mil](mailto:smbatnmci@mcsc.usmc.mil) or (703) 784-4898.

**NOTE:** The financial impact is significant for seats that individually request the release subsequent to its initial deployment. Requestors are charged for an SRM (MAC) or Distribution CLIN using the RRPTE process to have the application pushed to their desktops. A lack of application mapping does not stop the deployment of the application to the tier servers; it adds additional costs to the Government/Command to distribute the release to client workstations.

### **6.6.3.6 Application Mapping Submission Timeline**

#### **Planned Release**

Application mapping documentation must be submitted no later than Packaging & Certification process completion. The Navy NMCI PMO (NSCM) monitors and manages this timeline.

#### **Unplanned Release**

Application mapping documentation must be submitted no later than 7 days prior to Packaging & Certification process completion. The Navy NMCI PMO (NSCM) monitors and manages this timeline.

### **6.6.4 Finalize New or Updated DITSCAP Documentation**

The developer finalizes DITSCAP documentation and submits it to the Navy NMCI PMO NSCM or to the Marine Corps MCSC/EBSS for review and submission to the service NMCI DAA.

#### **6.6.5 Submit RDP**

The developer forwards the RDP to the Navy NMCI PMO NSCM or to the Marine Corps MCSC/EBSS for review and submission to the EDS APM. The NSCM reviews the RDP and ensures that all required documentation and information are present. Upon completion, the NSCM forwards the RDP for unclassified releases to the assigned APM and for classified releases to the NAVCOMTELSTA – NMCI NOC, Naval Air Station North Island.

##### **6.6.5.1 Planned Release**

The developer must submit the RDP for planned releases to the appropriate agency on or before the application completes packaging and certification.

##### **6.6.5.2 Unplanned Release**

The developer must submit the RDP for an unplanned release to the appropriate agency at the same time as the Application Submission Package is submitted to the Applications Lab for processing. If this does not occur, the release will not begin processing.



The overall goal of the NMCI program is for EDS to distribute all releases through a Novadigm Radia instance. Therefore, EDS uses a software management tool for deploying an enterprise solution, rather than loading locally.

### **6.7.1 Audit the Application Submission Packet**

The Audit process ensures the Application Submission Packet is complete and contains all the required information pertaining to the release. Once the packet is verified as being complete, the release continues through the remaining process steps. If the packet is determined to be incomplete, the release is removed from the process, the developer is notified of the discrepancy, and upon completion of corrective action, the release continues through the remaining process steps.

#### **6.7.1.1 Determine Raw Media or .msi Package**

EDS reviews the submitted media to determine whether it is raw media or an .msi instance. This supports the next step in the audit process to identify necessary action to complete EDS packaging of the media.

#### **6.7.1.2 Audit the msi Instance**

An .msi instance is audited to ensure that it is complete and ready for repackaging to create a Novadigm Radia instance.

#### **6.7.1.3 Package the .msi Instance and Raw Media to a Radia Instance**

A packet containing raw media is packaged to create a Novadigm Radia instance. In the event that the media cannot be packaged into a Novadigm Radia instance, the media is packaged as an .msi instance. If the media cannot be packaged into an .msi instance, it is returned to the developer for corrective action.

### **6.7.2 Radia Packaging**

EDS uses Novadigm Radia as the primary tool for packaging software to create an enterprise, site-specific, or customized instance. It enables EDS to automate the tasks associated with the management of software deployed on NMCI seats.

The primary objective is to deploy applications on an enterprise scale using the Navadigm Radia tool. However, sometimes, the software cannot be packaged using this tool at an enterprise level and must be deployed locally. The following paragraphs define a Push and the exception (a local load).

#### **6.7.2.1 Push**

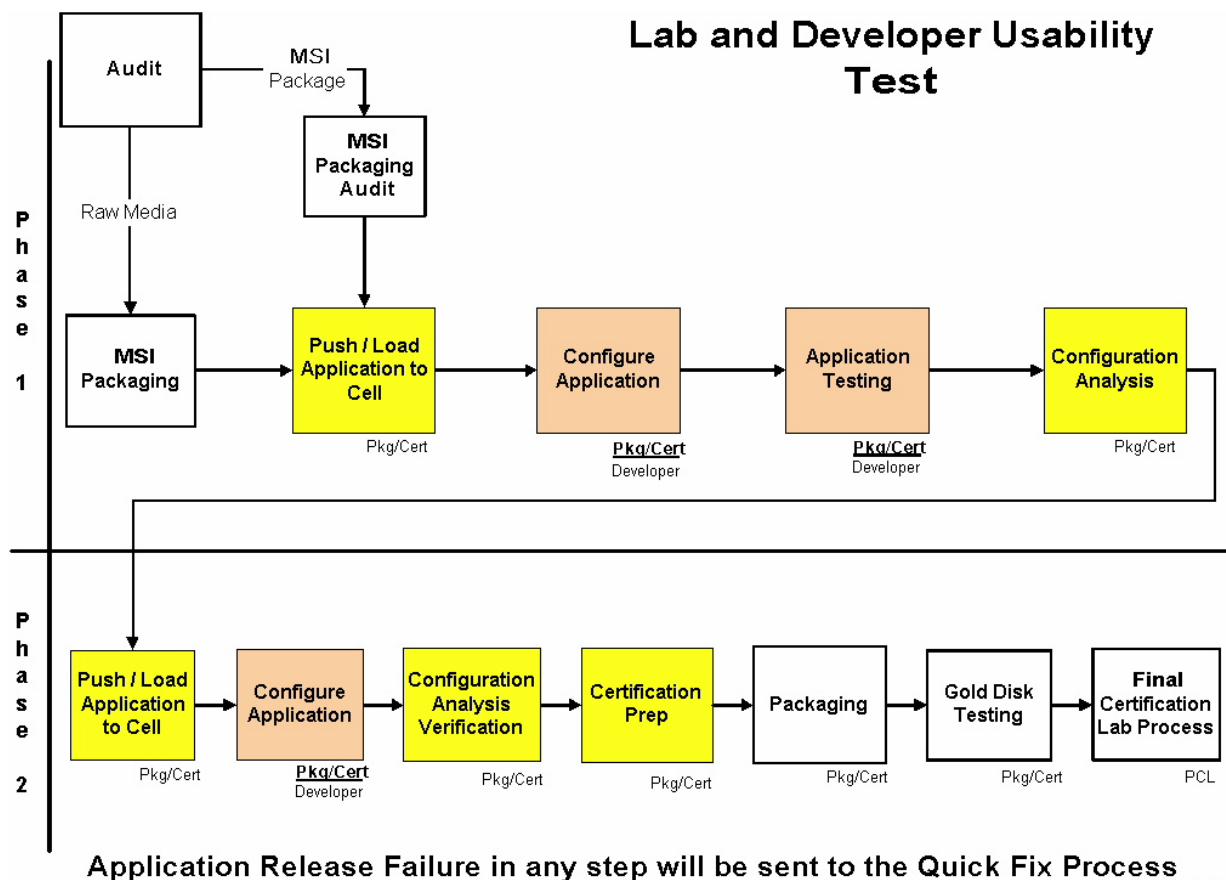
A Push is defined as the deployment of an application electronically from the NOC to the NMCI seat. This method is able to deploy an application across the enterprise and is the preferred means of deployment.

#### **6.7.2.2 Local Load**

A local load is used only as a last resort when an application fails to be packaged as a Radia instance for deployment. A local load option includes the installation of a release on the seat either manually or through a central server. Releases that are local loads must be packaged using Advanced Publisher to create an .msi. instance.

### 6.7.3 Lab and Developer Usability Test

Figure 6-11 depicts the Lab and Developer Usability Test process. The Usability Test verifies the IA compliance of the release, based on information obtained by the developer during the Collection and Submission process. When planned releases are being tested, the developer and/or designated representative must be available to help with problem solving through Quick Fix (Paragraph 6.7.5).



**Figure 6-11 Lab and Developer Usability Test**

The packaged release is tested in an NMCI-simulation test cell at the Applications Lab. The developer and/or designated representative assists with configuration changes required for installation and updates the supporting documentation.

The Applications Lab is responsible for completing the following tasks:

- Run network diagnostics tool using a sniffer (EtherPeek software) to trace the ports, protocols, and services used by the release.
- Document the test results.
- Send the test results to EDS IA.
- Review for compliance with B1 and B2 firewall policies.

## **Site Visit Request**

Developers or designated representatives who wish to participate in the Lab and Developer Usability Test at the EDS Applications Lab must complete a Site Visit Request. [Appendix I.5](#) describes the Site Visit Request requirements.

### **6.7.4 Gold Disk Testing**

All releases undergo Gold Disk Testing to preclude interoperability or compliance problems with the Gold Disk application loadset. If the release fails the Gold Disk Testing, it is sent to Quick Fix for problem resolution. When corrective action has been completed, the release is returned to Gold Disk Testing to validate the solution.

### **6.7.5 Quick Fix**

If a release fails the Lab and Developer Usability Test or Gold Disk Testing, it is sent to Quick Fix for resolution. The goal of the Quick Fix is to identify, analyze, and apply a rapid, easily applied solution for the release to meet final packaging and certification requirements. The Applications Lab and developer work together to identify a solution. After the solution is identified and applied, the release is returned to the Lab and Developer Usability Test or Gold Disk Testing process. Once the Quick Fix solution is validated, the developer updates the Release Deployment Solution Instructions. EDS then updates the release deployment documentation with the revised instructions.

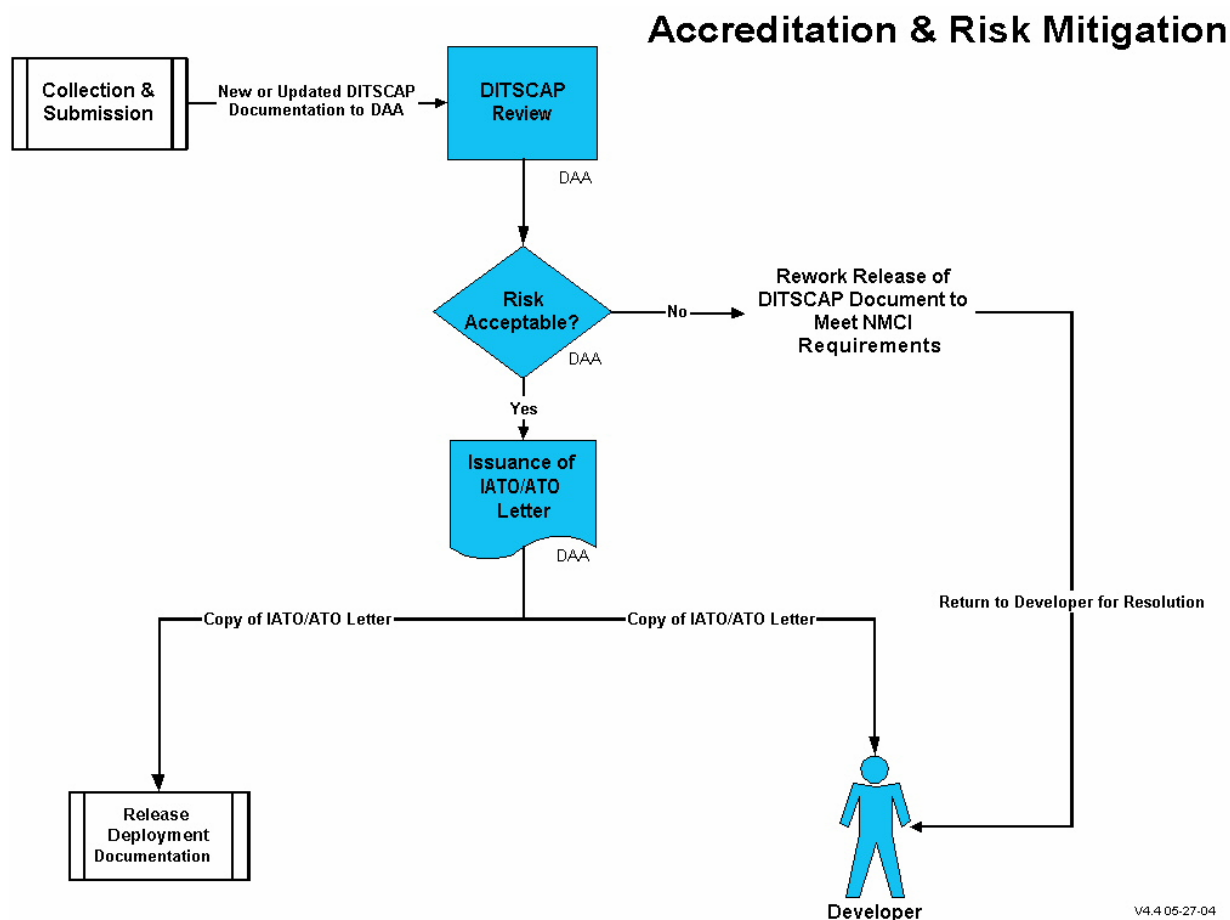
If a problem cannot be readily resolved at the Applications Lab, the release is returned to the developer for further action. If the developer still intends to deploy the release, the developer must correct the problem before resubmitting the release.

### **6.7.6 Final Certification Lab Process**

Once the release has successfully completed testing, the EDS Proving Center Lab (PCL) conducts a final review of the release and issues a certification letter. This letter is available for viewing in the ISF Tools Database. The Applications Lab forwards Novadigm Radia instances and local load software, including .msi instances, to the Definitive Software Library (DSL), pending release to the NOC. The PCL updates the release deployment documentation with the finalized release deployment instructions.

## **6.8 ACCREDITATION AND RISK MITIGATION**

Figure 6-12 depicts the Accreditation and Risk Mitigation process. All releases follow this process in accordance with the provisions contained in Paragraph [4.7](#).



**Figure 6-12 Accreditation and Risk Mitigation**

During this process, the service NMCI DAA completes the following tasks:

- Review DITSCAP documentation.
- Grant certification.

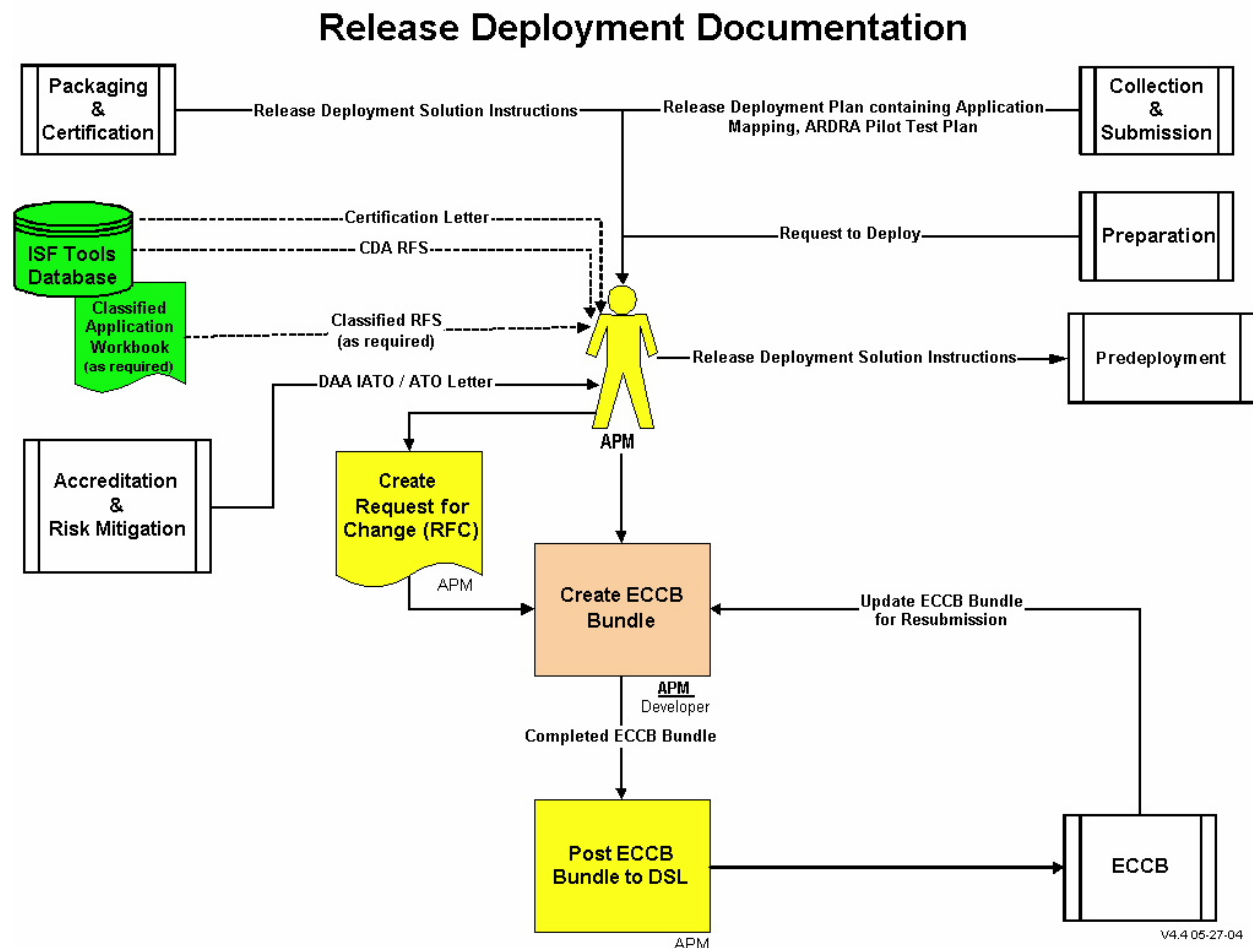
During the Collection and Submission process, the developer submitted all required DITSCAP documentation to the service NMCI DAA for review and approval. The service NMCI DAA reviews the DITSCAP documentation and assesses the IA impact (risks to the network and desktop) of the release to

If the service NMCI DAA deems the risk acceptable, an IATO/ATO is granted to operate within the NMCI environment. If the service NMCI DAA determines that the risk is unacceptable, the DITSCAP documentation is returned to the developer for rework and resubmission.

The service NMCI DAA ensures that a copy of the IATO/ATO letter is provided for inclusion in the release deployment documentation.

## 6.9 RELEASE DEPLOYMENT DOCUMENTATION

Figure 6-13 depicts the release deployment documentation to support the continual collection of information and documentation pertaining to the release as it undergoes the NRDP.



**Figure 6-13 Release Deployment Documentation**

This process includes the following tasks:

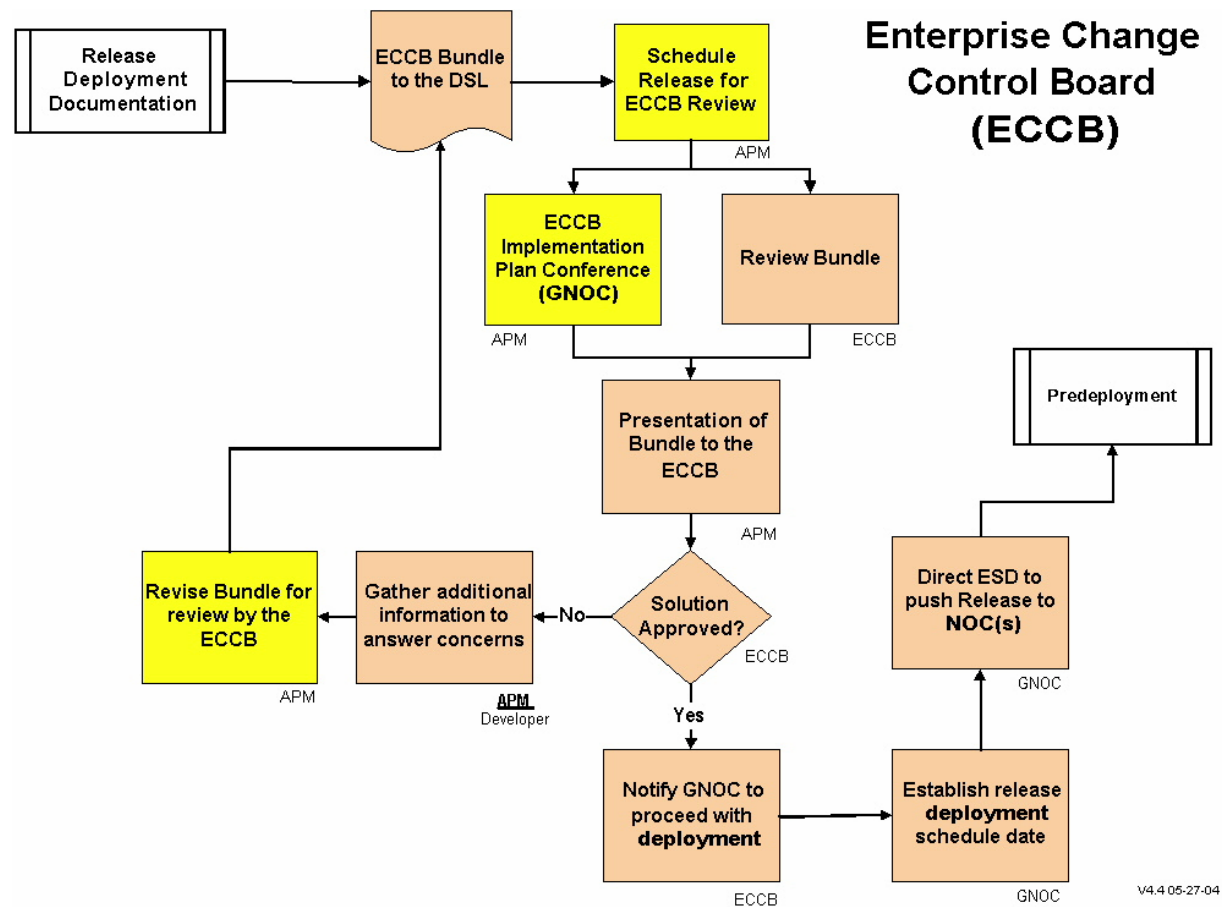
- Update existing documentation.
- Create an ECCB bundle.
- Post the ECCB bundle to the DSL.

The APM maintains all release deployment documentation until the release has been fully deployed in NMCI, at which time it is stored in the DSL. As can be seen, a variety of information is gathered from many sources throughout the NRDP in order to prepare the many documents necessary to support the deployment of a release. A critical step in this process is development of the ECCB bundle by the APM. The ECCB bundle consists of the following documents:

- Request for Change (RFC).
- Release Deployment Solution Instructions
- Release Deployment Plan (RDP)
- DAA IATO/ATO Letter
- ARDRA/Pilot Test Plan

## 6.10 ECCB

Figure 6-14 depicts the ECCB process for review and approval of a release to deploy within NMCI. The ECCB is composed of representatives from the Navy, Marine Corps, Navy NMCI PMO, and EDS. IA and operations representatives from the Navy and Marine Corps work with EDS and Navy NMCI PMO to assess the business and technical properties of the release.



**Figure 6-14 Enterprise Change Control Board (ECCB)**

The ECCB also determines whether the application poses a risk to the NMCI operational environment once it is deployed to the desktop. The ECCB reviews the bundle and approves releases that meet all NMCI requirements.

The release is scheduled for presentation to the ECCB in accordance with its weekly scheduling process.

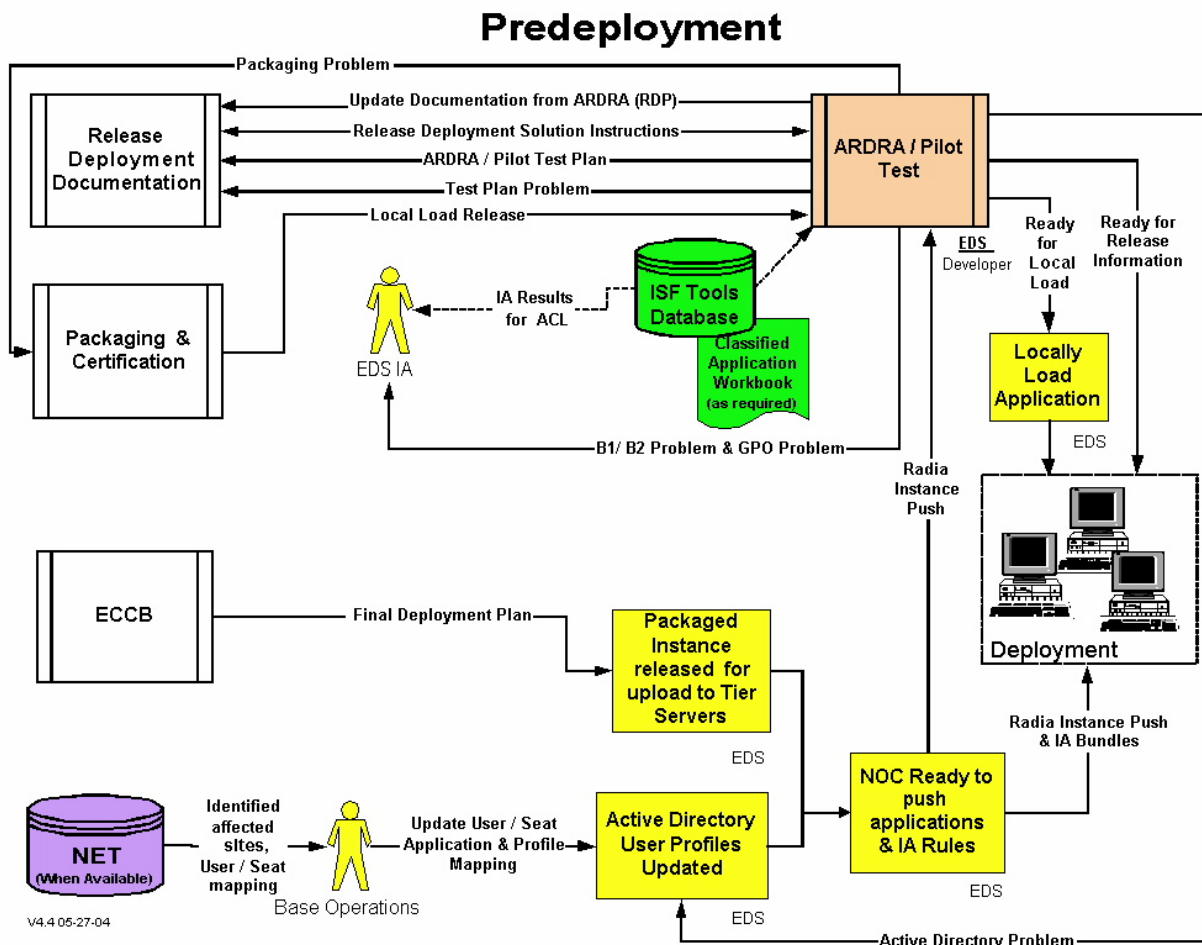
If the release is approved, the ECCB notifies the Global Network Operations Center (GNOC) to proceed with the deployment. The GNOC establishes a deployment schedule date and directs the ESD to push the release to the NOCs.

If the release is disapproved, the ECCB bundle is returned to the APM for corrective action. The APM passes this requirement to the CCS if developer support is needed. Once corrective action has been completed, the APM revises the ECCB bundle and schedules an ECCB review.



## 6.11 PREDEPLOYMENT

Figure 6-15 depicts the Predeployment process, which is primarily an EDS responsibility. This process completes final preparations for deployment in accordance with the Application Mapping Plan.



**Figure 6-15 Predeployment Process**

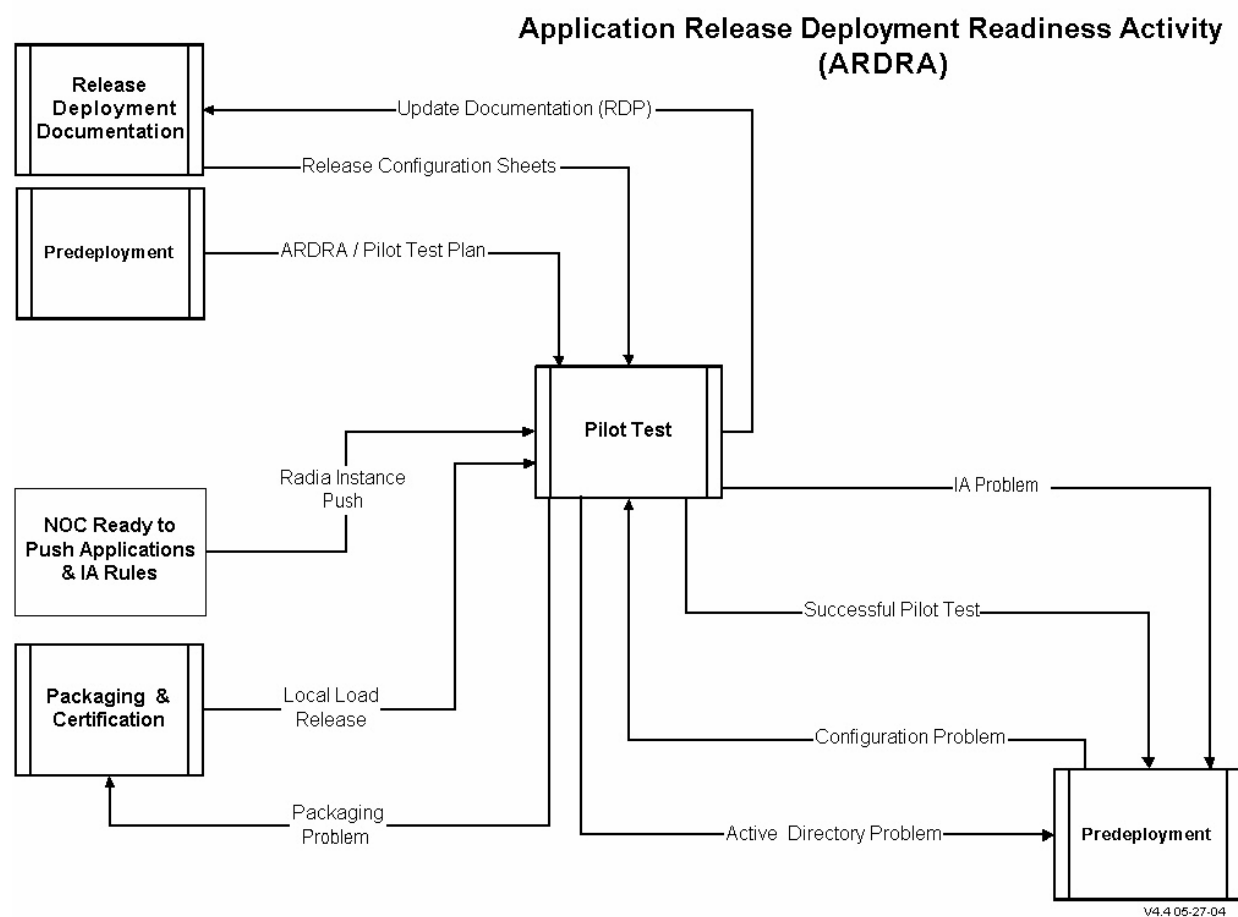
Before ARDRA/Pilot Test can begin, EDS must ensure completion of the following milestones:

- Enterprise B1 is in place at the NOC.
- Enterprise B2 and GPO are deployed.
- Final Deployment Plan is completed.
- Release Deployment Solution Instructions are ready.
- Local deployment releases are ready.
- NOC is ready to push releases to NMCI seats. This includes two tasks:
  - GNOC loads Radia instances from the DSL to the San Diego NOC and uploads to the designated NOC.
  - Base Operations updates the user profiles in the AD using the sites, servers and user-mapping information received from the developer to conduct the ARDRA/Pilot Test.

For classified applications, the Classified Application Workbook stores classified or sensitive information that cannot be stored in the ISF Tools Database.

## 6.12 APPLICATION RELEASE DEPLOYMENT READINESS ACTIVITY (ARDRA)

Figure 6-16 depicts ARDRA, which is the final evaluation of the release prior to deployment. ARDRA verifies the final release configuration, NOC connectivity, and boundary policies prior to deployment.



**Figure 6-16 Application Release Deployment Readiness Activity (ARDRA)**

The ARDRA/Pilot Test verifies and validates the deployability and functionality of the release in a live NMCI environment prior to full deployment of the release. ARDRA has the following objectives:

- Evaluate the performance and IA policies of certified DSL releases. This can include unclassified/classified COTS and GOTS in a true NMCI production environment.
- Provide on-the-job-training for select NMCI seat deployment and EDS base operations personnel on the manual configuration of a release.
- Ensure proper network configuration and operations.

- Evaluate migration tools.
- Evaluate Radia applications management.
- Validate migration implementation plan and test print functions.

EDS, with input from the developer, decides whether to conduct an ARDRA/Pilot Test for the release. Generally, the ARDRA/Pilot Test is only used to test and evaluate complex applications. The ARDRA/Pilot Test can also be conducted on simple applications if EDS and the developer determine this requirement is necessary to ensure successful deployment. EDS Base Operations conducts the ARDRA/Pilot Test in the live NMCI environment. The ARDRA/Pilot Test can be used on classified and unclassified networks and on COTS and GOTS software.

### **6.12.1 ARDRA/Pilot Test Plan**

The key to the success of the ARDRA/Pilot Test is a well designed plan. This requires commitment from appropriate Commands, planning for availability of personnel and equipment, but most importantly, communications between all parties, including EDS, developer, affected customers, and Commands. The developer must develop an ARDRA/Pilot Test Plan well in advance of the start of the test. (Refer to the ARDRA/Pilot Test checklist in [Appendix I.6.](#))

The developer should understand the purpose and methodology of the plan and be conversant on its objectives. The developer should be in very close communications with the EDS Application Program Manager in order to mitigate any unforeseen issues.

The ARDRA/Pilot Test Plan must include the following items:

- Scope, strategy, and timeline
- Commands and environment requirements
- Tools and test equipment required
- Roles and responsibilities
- Recovery and error-handling tests
- Testing criteria
  - Test descriptions
  - Pilot install and criteria to begin testing
  - Configuration tests
  - Functional tests
  - Load and performance tests
  - Stress tests
- Problem recording, issues management and escalation, rework, and resolution
- Exit criteria

### **6.13 ARDRA/PILOT TEST**

Figure 6-17 depicts a preferred methodology to process the final ARDRA/Pilot Test. After Predeployment activities are completed, the developer and EDS must complete the ARDRA/Pilot Test in order to release the application.



If the Radia instance push was successful, the developer and test group continue to evaluate the release, as detailed in the ARDRA/Pilot Test Plan. EDS and the developer, again jointly, verify success or failure of the test. If a failure has been discovered, a failure analysis determines the level of the failure. If the failure can be corrected within the constraints of the test, the corrections are implemented and the test continues to completion. If the failure cannot be corrected within the constraints of the test, the Backout Plan must be initiated, errors documented, and the release returned to the developer for reengineering. If the test is successful, the process continues until ARDRA/Pilot Test completion. The results of the ARDRA/Pilot Test are documented and forwarded to the APM for inclusion with all other documentation pertaining to the release.

## 6.14 DEPLOYMENT

Once the ARDRA/Pilot Test has been implemented and documented, the application is pushed to the NOC in accordance with the RDP. The NMCI Electronic Software Delivery model assumes that users leave their computers turned **ON** during the night so as to be available for frequent, and often large, software updates. When large groups of users turn their computers off, these updates cannot occur when scheduled, and by design, are postponed until a user logs in the next morning. This practice causes potentially significant delays at entire sites during the first few hours of the work day as large numbers of users log into the network at approximately the same time.

If you know in advance that you are on distribution for an application and it does not deploy to you, contact the Help Desk.

### Required Actions:

- Do **NOT** turn off your computer at night. Leave your computer powered on when you leave at the end of the work day.
- You may restart your NMCI seat every night before you leave, but please do not shut down the NMCI seat completely, and **never leave your NMCI seat logged in overnight.**
- Laptop users who use docking stations are encouraged to leave the laptop locked in the docking station as often as possible. Leaving the laptop turned **ON** in the docking station at night increases its chances of receiving updates successfully and reduces user impact during work hours.

## APPENDIX A: GLOSSARY OF ACRONYMS AND TERMS

Term	Definition
A&RM	Accreditation and Risk Mitigation
ACTR	Activity Contract Technical Representative. A designated person on the MAC Authorized Submitter List.
AD	Active Directory
ADS	Authoritative Data Source
ADSI	Active Directory Service Interface
Agent Software	Any software that monitors and/or captures network traffic or queries network nodes for the purpose of reporting the captured information back to the user or another network node. This type of information is considered sensitive and its capture and dissemination poses a security risk.
AIS	Automated Information Systems
AIT	Application Integration and Testing
AOR	Assumption of Responsibility: The date when responsibility for operating the “as-is” environment and for work defined by the ordered NMCI Contract Line Item Number (CLIN) shifts from the Government and its local contractors to the Integrated Solution Framework (ISF).
API	Application Program Interface
APM	Application Project Manager
Application	(1) An automated software program that collects, stores, processes, and/or reports information in support of a specific user requirement. (2) Any software program that runs in a server-based or standalone environment that is used in a production capacity.
Application Development Software	Any software that generates or allows the user to create programming code which complies with executable (.exe) files that are installed and can be run from the user’s workstation. Application Development Software is only permitted to reside on Science and Technology (S&T) seats.
Application Survey	The process of gathering commercial off the shelf (COTS) and Government off the shelf (GOTS) application information necessary to rationalize or certify applications for migration to the NMCI environment. The three categories of applications surveys are (1) desktop: a single user application not on the standard NMCI seat, (2) server-based, and (3) web-based.
ARDRA	Application Release Deployment Readiness Activity
ARG	Application Resources Guide
ASN RDA	Assistant Secretary of the Navy for Research Development and Acquisition
ATO	Authority to Operate
B1	Boundary 1
B2	Boundary 2
B3	Boundary 3
B4	Boundary 4
BLII	Base Level Information Infrastructure
BOM	Base Operations Manager
C&A	Certification and Accreditation: The comprehensive evaluation of the technical and non-technical security features of an information system and other safeguards, made in support of the accreditation process, to establish the extent to which a particular design and

Term	Definition
	implementation meets a set of specified security requirements. <i>Source: National Security Telecommunications and Information Systems Security Instruction (NSTISSI) 4009, National Information Systems Security (INFOSEC) Glossary.</i> Includes testing the ability of the application to electronically distribute.
CAL	Complex Application Laboratory
CCS	Central Design Activity (CDA) Customer Support
CDA	Central Design Activity (Navy only). This document uses the term “developer” to denote the inclusion of the Marine Corps.
CIO	Chief Information Officer
Client	The client part of <i>client-server architecture</i> . Typically, a client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an <i>e-mail client</i> is an application that enables you to send and receive e-mail.
CLIN	Contract Line Item Number
CM	Configuration Management
CNO	Chief of Naval Operations
CPDA	Classified Product Delivery Analyst
COI	Communities of Interest
Command	A Navy claimant or Echelon II or Marine Corps Forces Command (i.e., MARFORPAC, MARFORLANT, and MARFORRES).
Common Portal Services	The logical set of common portal functions and services exposed and available to the user facing service developer.
Content	The text, graphics, audio, video, services, and applications available at a web site.
COTS	Commercial Off the Shelf
Cutover	The actual event of rolling out NMCI desktops. Cutover follows the preparation phases of pre-AOR and post-AOR of the legacy applications transition. <u>Cutover Start</u> : In theory, Cutover begins at the predesignated time when all precutover transition work is complete. Cutover actually begins upon the rollout of the first NMCI desktop at a site. <u>Cutover Complete</u> : In theory, Cutover is complete when the final desktop and application are successfully deployed. In actuality, Cutover ends at the successful rollout of the last scheduled desktop.
CTR	Contract Technical Representative. A designated person on the MAC Authorized Submitter List.
DAA	Designated Approval Authority
DADMS	Department of the Navy Application Database Management System
Deployment	The delivery of an authorized application to a designated server or desktop through an automated or local deployment process.
Developer	A person who either develops or supports introduction software of NMCI. This also includes consumers, software vendors, application owners, Program of Record-Program Manager (POR-PM), and Commands that sponsor software.
DISA	Defense Information Systems Agency
DITSCAP	Department of Defense (DoD) Information Technology Security Certification and Accreditation Process
DMZ	Demilitarized Zone
DoD	Department of Defense
DON	Department of the Navy
DOS	Data Oriented Service: A software component that receives a request and optionally returns

<b>Term</b>	<b>Definition</b>
	an extensible markup language (XML) data response. DOS may interact with common portal services and other services published in the Service Registry.
DS	Directory Services
DT&E	Developer Test and Evaluation
EAGLE	Enterprise Applications Group for Legacy and Emerging
EBSS	Enterprise Business Systems Support
ECCB	Enterprise Change Control Board
EDM	Enterprise Desktop Manager
EDS	Electronic Data Systems
DSL	Definitive Software Library
Enterprise	Literally, a business organization. In the computer industry, the term is often used to describe any large organization that uses computers. An intranet, for example, is a good example of an enterprise computing system. In this case, the entire NMCI environment.
ERQ	Engineering Review Questionnaire
FA	Functional Area
FAM	Functional Area Manager
FAQ	Frequently Asked Question
FDA	Functional Data Administrator
FDM	Functional Data Manager
FFP	Fleet Firewall Policy
FNC	Functional Namespace Coordinator
GFI	Government Furnished Information
GIG	Global Information Grid
GNOC	Global Network Operations Center
GOTS	Government Off the Shelf
GPO	Group Policy Object: A collection of settings that define what a system will look like and how it will behave for a defined group of users. GPO is associated with selected Active Directory containers, such as sites, domains, or organizational units (OUs).
HI	Horizontal Integration
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
I&A	Identification and Authentication
IA	Information Assurance
IATO	Interim Authority to Operate
IATT	Information Assurance Tiger Team
IAVA	Information Assurance Vulnerability Alert
ID	Identification
IE	Internet Explorer
IM	Information Management
INFOSEC	Information Security
IP	Internet Protocol
ISF	Integrated Solution Framework (Tools Database)
IT	Information Technology



<b>Term</b>	<b>Definition</b>
ITI	Inspection/Test Instruction
IT/IM	Information Technology/Information Management
IT-21	Information Technology for the 21st Century
Java	A general purpose, high-level, object-oriented, cross-platform programming language developed by Sun Microsystems [not an acronym].
JSP	Java Server Pages
LADRA	Legacy Application Deployment Readiness Activity
LAPOC	Legacy Application Point of Contact
LATG	Legacy Application Transition Guide
LDAP	Lightweight Directory Access Protocol
LDE	Limited Deployment Evaluation
Legacy Application	An existing customer software application that is not included in the NMCI standard seat services or the Contract Line Item Number (CLIN) 0023 catalog.
Local Deployment	The act of manually loading an authorized client application to the NMCI seat.
LSTG	Legacy Systems Transition Guide
LHSP	Lifecycle Help Desk Support Plan
MAC	Move, Add, Change
MCAIT Lab	Marine Corps Applications Integration Testing Laboratory
MCTN	Marine Corps Tactical Network
Metadata	Metadata consists of information that characterizes data. It documents data products. That is, metadata answers who, what, when, where, why, and how about the data being documented; how and when and by whom a particular set of data was collected, and how the data is formatted. Metadata is essential for understanding information stored in data warehouses.
MS	Microsoft
.msi	Microsoft Windows Installer
NADTF	Navy Applications Database Task Force
NAVNETWARCOM	Naval Network Warfare Command
NAVSEA	Naval Sea Systems Command
Deputy CIO (Navy)	Navy Information Officer
NEADG	Navy Enterprise Application Development Guide
NEP	Navy Enterprise Portal: The logical set of functional components that comprise the central portal infrastructure, including the Portal, the Service Registry and the Common Services. The gateway to the Navy Enterprise Portal is <a href="https://www.homeport.navy.mil/">https://www.homeport.navy.mil/</a> .
NET	NMCI Enterprise Tool
NIPRNET	Non-Secure Internet Protocol Router Network
NMCI	Navy Marine Corps Intranet
NNWC	Naval Network Warfare Command
NOC	Network Operations Center
NRDDG	NMCI Release Development and Deployment Guide
NRDP	NMCI Release Deployment Process
NRPM	NMCI Release Prioritization Manager
NRSM	NMCI Release Schedule Manager
NSCM	NMCI Software Configuration Manager

<b>Term</b>	<b>Definition</b>
OCONUS	Outside Continental United States
OU	Organizational Unit
PEO-IT	Program Executive Office for Information Technology
PG	Product Group
PIV	Project InVision
PKE	Public Key Enabled
PKI	Public Key Infrastructure
PM	Program Manager
PMO	Program Management Office
POC	Point of Contact
POP	Point of Presence
POR-PM	Program of Record-Program Manager
Portal	The functional component of the Navy Enterprise Portal that is responsible for aggregating portlets.
Portal Client	A software application or hardware device that communicates with the Navy Enterprise Portal using the Portal Client Interface. Includes the set of web browsers, developers, and mobile devices.
Portal Client Interface	A Hypertext Transfer Protocol (HTTP) Request/Response initiated by a portal client to the Navy Enterprise Portal.
Portal Service Response	A response sent from a common portal service to a user-facing service
Portlet	The visible, active windows that end-users see within their Enterprise Portal interface.
PPL	Preferred Products List
QAPs	Quarantined Applications
Q-RDA	Quarantined Upgrade Emerging Support Team (QUEST) Release and Deployment Analyst
Q-RDT	Quarantined Upgrade Emerging Support Team (QUEST) Regional Deployment Team
QUEST	Quarantined Upgrade Emerging Support Team
RDP	Release Deployment Plan: The RDP provides a complete history of the release from inception through deployment. It contains all documentation used throughout the process, including reengineering or fixes made to satisfy testing and compliance requirements. The plan also documents if certain functions of the release do not work. The developer is responsible for the development and maintenance of the plan. The developer should use existing documentation where possible, and only create or capture information not previously available.
RFC	Request for Change
RFS	Request for Service
RRPTE	Requesting Release in the Post-Transition Process Environment: A site that has completed Cutover or is operating in the post-transition environment uses RRPTE to obtain a release that has already been tested and certified and is ready for deployment in the NMCI environment.
RTD	Request to Deploy: The only authorized means for approving and deploying a release into NMCI. Naval Network Warfare Command (NNWC) is the designated approval authority for all releases submitted for deployment. The NMCI Release Prioritization Manager (NRPM) and NMCI Release Scheduling Manager (NRSM) meet quarterly to process submitted RTDs for deployment during the next three quarters. The two types of RTDs are Planned Release and Unplanned Release. <u>Planned Release:</u> The fundamental process for submitting periodic updates to existing applications, testing certification deployment of quarantined solutions, and introducing new

Term	Definition
	(emerging) applications. <u>Unplanned Release</u> : Supports deployment of release that requires expedited handling to repair an application that cannot perform its intended function.
S&T	Science and Technology
SCM	Software Configuration Management
Service Registry	The functional component of the Navy Enterprise Portal that stores metadata on user-facing and data-oriented services.
SGML	Standard Graphical Markup Language
SIPRNET	Secure Internet Protocol Router Network
SLA	Service Level Agreement
SM	Site Manager
SME	Subject Matter Expert
SNAC	Systems and Network Attack Center
SOAP	Simple Open Access Protocol
SOC	Security Operations Center
SPAWAR	Space and Naval Warfare Systems Command
SSL	Secure Socket Layer
TB	Transport Boundary
TFW	Task Force Web
TO	Task Order
UDDI	Universal Description Discovery and Integration
UFS	User Facing Service: A software component that receives a UFS Request from the portal and returns an UFS Response that formats the content for display (usually in a markup language such as HTML or WML) to produce visual output in a Portlet. A User-Facing Service may interact with Common Portal Services and other Services published in the Service Registry.
UFS Request	A request sent to a User Facing Service (UFS) from the Navy Enterprise Portal. Currently, the two types of UFS Requests are Hypertext Transfer Protocol (HTTP) Request and HTTP Simple Open Access Protocol (SOAP) Request.
UFS Response	A response sent to the Navy Enterprise Portal from a UFS.
UNC	Universal Naming Convention
UPN	User Principal Name
URL	Uniform Record Locator
USMC	United States Marine Corps
VBNS+	Very High Speed Backbone Network Service
VPN	Virtual Private Network
WAN	Wide Area Network
Web Service	A software component that is described through WSDL, can be published and located in a Universal Description Discovery and Integration (UDDI) Registry, and is invoked through Simple Open Access Protocol (SOAP) over Hypertext Transfer Protocol (HTTP).
WIT	Waiver Input Template
WML	Wireless Markup Language
WSDL	Web Services Definition Language
WSE	Web Service Execution
WSEE	Web Service Execution Engine

<b>Term</b>	<b>Definition</b>
WSRP	Web Services for Remote Portal
WWW	World Wide Web
XML	Extensible Markup Language: A simple, very flexible text format derived from Standard Graphical Markup Language (SGML) (International Standards Organization - ISO 8879). Originally designed to meet the challenges of large-scale electronic publishing, XML is also playing an increasingly important role in the exchange of a wide variety of data on the web and elsewhere.

## APPENDIX B: HYPERLINKS, NAVY MESSAGES, AND DOCUMENTS

### Hyperlinks

Topic	URL
Browser Security	<a href="http://iase.disa.mil/policy.html">http://iase.disa.mil/policy.html</a>
Certification and Accreditation (C&A)	<a href="http://iase.disa.mil/ditscap/index.html">http://iase.disa.mil/ditscap/index.html</a>
Certified for Windows Program	<a href="http://msdn.microsoft.com/certification">http://msdn.microsoft.com/certification</a>
DADMS	<a href="https://www.dadms.navy.mil">https://www.dadms.navy.mil</a>
Directory and Registry Permissions	<a href="http://www.microsoft.com/windows2000/">http://www.microsoft.com/windows2000/</a>
DISA Information Systems Center (DISC)	<a href="http://www.disa.mil/disc/disc.html">http://www.disa.mil/disc/disc.html</a>
DoD Mobile Code Policy	<a href="http://www.c3i.osd.mil/org/cio/doc/mobile-code11-7-00.html">http://www.c3i.osd.mil/org/cio/doc/mobile-code11-7-00.html</a>
DoD Policy for Web Content	<a href="http://www.defenselink.mil/webmasters">http://www.defenselink.mil/webmasters</a>
FAM Application Waiver Process	<a href="https://www.dadms.navy.mil/?IndexID=40">https://www.dadms.navy.mil/?IndexID=40</a>
Firewall Policies	<a href="https://infosec.navy.mil">https://infosec.navy.mil</a>
Form or Distribution CLIN	<a href="http://www.nmci-isf.com/helpdesk_reqforms.asp">http://www.nmci-isf.com/helpdesk_reqforms.asp</a>
INFOSEC Web Site	<a href="https://infosec.navy.mil">https://infosec.navy.mil</a>
ISF Tools Database	<a href="http://www.nmci-isf.com/transition.htm#Legacy">http://www.nmci-isf.com/transition.htm#Legacy</a>
Legacy Applications Liaison Updates	<a href="https://tfw-opensource.spawar.navy.mil">https://tfw-opensource.spawar.navy.mil</a> (under contacts) <a href="http://www.nmci-isf.com/">http://www.nmci-isf.com/</a>
Legacy Applications Transition Guide	<a href="http://www.nmci-isf.com/legacy_applications_transition_guide.pdf">http://www.nmci-isf.com/legacy_applications_transition_guide.pdf</a>
Mail-Enabled Public Folder	<a href="http://msdn.microsoft.com/">http://msdn.microsoft.com/</a>
Microsoft Developer Network (MSDN)	<a href="http://msdn.microsoft.com/">http://msdn.microsoft.com/</a>
Microsoft Development Standards	Desktop Spec: <a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli.asp</a> Server Spec: <a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2ksrv/html/w2ksrv.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2ksrv/html/w2ksrv.asp</a>
Navy Enterprise Application Deployment Guidance (NEADG)	<a href="https://neadg.spawar.navy.mil/idg/view/home.do">https://neadg.spawar.navy.mil/idg/view/home.do</a> REQUIRED PKI SPONSOR AND EMAIL.
Network Related APIS other than Standard WIN2K APIS	<a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adsi/active_directory_service_interfaces_atsi.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/adsi/active_directory_service_interfaces_atsi.asp</a>
NMCI Legacy Systems Support CLIN 0029	<a href="http://www.nmci-isf.com/clin029.htm">http://www.nmci-isf.com/clin029.htm</a>
NMCI Public Key Infrastructure & Directory System	<a href="https://infosec.navy.mil">https://infosec.navy.mil</a>
NMCI Public Web Site	<a href="http://www.nmci-isf.com/">http://www.nmci-isf.com/</a>
NMCI Release Deployment Process (NRDP)	<a href="https://usplswebh0ab.plano.webhost.eds.net/isftool/Login.jsp">https://usplswebh0ab.plano.webhost.eds.net/isftool/Login.jsp</a>
NMCI Ruleset (NADTF)	<a href="http://cno-n6.hq.navy.mil/navcio/leg_apps.htm">http://cno-n6.hq.navy.mil/navcio/leg_apps.htm</a>
NMCI Science and Technology Desktop Configuration CLIN 0038	<a href="http://www.nmci-isf.com/clinlist.htm">http://www.nmci-isf.com/clinlist.htm</a>
NMCI Server Connectivity CLIN 0027	<a href="http://www.nmci-isf.com/clinlist.htm">http://www.nmci-isf.com/clinlist.htm</a>

Topic	URL
NMCI Standard Desktop Configuration CLIN 0001-0004	<a href="http://www.nmci-isf.com/clin_matrix.xls">http://www.nmci-isf.com/clin_matrix.xls</a> <a href="http://www.nmci-isf.com/clinlist.htm">http://www.nmci-isf.com/clinlist.htm</a> <a href="http://www.microsoft.com/windows2000/server/howtobuy/upgrading/compat/">http://www.microsoft.com/windows2000/server/howtobuy/upgrading/compat/</a>
NMCI Transition	<a href="http://www.nmci-isf.com/transition.htm">http://www.nmci-isf.com/transition.htm</a>
Optional User Capabilities Catalog CLIN 0023	<a href="http://www.nmci-isf.com/clin023.htm">http://www.nmci-isf.com/clin023.htm</a>
OSD Deskbook Reference Library	<a href="http://web1.deskbook.osd.mil/htmlfiles/DBY_dod.asp">http://web1.deskbook.osd.mil/htmlfiles/DBY_dod.asp</a>
Plug-Ins Provided on Gold Disk	<a href="http://www.nmci-isf.com/downloads/Gold_disk_contents.pdf">http://www.nmci-isf.com/downloads/Gold_disk_contents.pdf</a>
Request to Deploy	Navy: <a href="http://www.nmci.navy.mil">www.nmci.navy.mil</a> Marine Corps: <a href="http://www.nmciinfo.mcsc.usmc.mil">www.nmciinfo.mcsc.usmc.mil</a>
Review CLIN 0023 Catalog Applications	<a href="http://www.nmci-isf.com/">http://www.nmci-isf.com/</a>
Science and Technology (S&T) Seat	<a href="http://www.nmci-isf.com/userinfo_sandtguide.htm">http://www.nmci-isf.com/userinfo_sandtguide.htm</a> <a href="http://www.nmci-isf.com/clinlist.htm">http://www.nmci-isf.com/clinlist.htm</a>
Terminal Services	<a href="http://www.microsoft.com/technet/">http://www.microsoft.com/technet/</a>
Windows 2000 Desktop Application Interface Specification	<a href="http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli.asp">http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli.asp</a>

## Navy Messages #12

Originator	Message Date Time Group (DTG)	Subject
CNO Washington DC//N09T/N1/N2/N3/N4/N6/N7/N8/ N093/N095/N096	R 252250Z FEB 02	NMCI Legacy Applications Transition Process
PEO IT Washington DC	R 261800Z FEB 02	Enterprise Legacy Application Management
CNO Washington DC//N09T/N09W	R 171442Z APR 02 NAVADMIN 007/01	Navy Enterprise Portal
CNO Washington DC	R 232208Z MAY 02	Enterprise Strategy for Managing Application Databases Within the Navy
CONSPAWARSYSCOM San Diego CA//PMW164-3	R 242225Z MAY 02	NMCI Process Summit Agreements
CNO Washington DC//N6N7	R 301245Z SEP 02	Enterprise Strategy for Managing NMCI Applications and Databases
CNO Washington DC//N6N7	R 071718Z OCT 02	Navy Standard Applications
COMNAVNETWARCOM Norfolk VA	R 131248Z DEC 02	Software Version Control
CNO Washington DC//N6N7	R 231700z DEC 02	NMCI Application Rule Set Action
CNO Washington DC//N09	R 252230Z JUL 03	Enterprise Strategy for Managing NMCI Applications and Databases Within NMCI
DON CIO Washington DC	R 261500Z AUG 03	Process for Release of Applications into NMCI Environment
COMNAVNETWARCOM Norfolk VA//N6	R 141945Z NOV 03 NIA 11-03	Clarification of DAA Policy for Certification and Accreditation of Applications on NMCI
COMNAVNETWARCOM Norfolk VA	R 051645Z DEC 03	Personal Digital Assistant Policy (PDA)
COMNETWARCOM Norfolk VA	R261420Z FEB 04	Maximum Email File Size

Originator	Message Date Time Group (DTG)	Subject
COMNAVNETWARCOM Norfolk VA	R 271618Z	NMCI Legacy Application/RTD Cancellation and Resubmission
COMFLTFORCOM Norfolk VA	R 031759Z	Legacy Application Reduction And Standardization In LANTFLT and PACFLT

## Instructions and Documents

Instruction / Document	Date	Subject
DoD5000.2-R	15 March 1996	Mandatory Procedures for Major Defense Acquisition Program (MDAPs) and Major Automated Information System (MAIS)
DoD 5200.28	21 March 1988	Security Requirements for Automated Information Systems (AISs)
DoD 8510.1-M	31 July 2000	DoD Information Technology Security Certification and Accreditation Process-DITSCAP Application Manual
DoD 4630.5	11 January 2002	Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)
Under Secretary of the Navy Letter	14 May 2002	Designation of Department of the Navy (DON) Functional Area Managers
Director NMCI/NETWARCOM Joint Letter	Undated	Navy Marine Corps Intranet Release Development and Deployment Guide
FAM Process		FAM Mid-Term Rationalization Guide v7.7
U.S. Navy	20 June 2002	Class 3 Public Key Infrastructure (PKI) Code Signing Attribute Authority (CSAA) Standard Operating Procedures (SOP) Version 1.0
Naval Research Laboratory	29 September 2001	Mobile Code/Object Certification Implementation Evaluation Document
Naval Research Laboratory	30 August 2002	PKI/Mobile Code Object Signing Evaluation Document

## APPENDIX C: POINTS OF CONTACT

Position/Billet	Email	Phone
<b>NMCI Program Managers Office (PMO)</b>		
Legacy Systems Division Director	<a href="mailto:peter.almazan@navy.mil">peter.almazan@navy.mil</a>	(858) 524-7435
EAGLE Team Lead	<a href="mailto:Joe.Dundas@navy.mil">Joe.Dundas@navy.mil</a>	(858) 537-8527
<b>NAVY CIO and NADTF</b>		
Director NADTF	<a href="mailto:ron.sticinski@navy.mil">ron.sticinski@navy.mil</a>	(202) 764-2942
Member NADTF	<a href="mailto:judy.Kelly@navy.mil">judy.Kelly@navy.mil</a>	(202) 764-1813
Member NADTF	<a href="mailto:cynthia.corman@navy.mil">cynthia.corman@navy.mil</a>	(202) 764-0852
Member NADTF	<a href="mailto:warren.hedin@navy.mil">warren.hedin@navy.mil</a>	(202) 764-0012
Member CIO	<a href="mailto:rodeck.renee@hq.navy.mil">rodeck.renee@hq.navy.mil</a>	(703) 604-6880
Member CIO	<a href="mailto:Downing.Christine@hq.navy.mil">Downing.Christine@hq.navy.mil</a>	(703) 604-8390
<b>Electronic Data System (EDS)</b>		
NMCI Help Desk Phone (Toll free)		(866) 843-6624
Application Project Manager (APM)	<a href="mailto:Edward.Lapating@eds.com">Edward.Lapating@eds.com</a>	(619) 817-3458
Classified Product Delivery Analyst (CPDA)	<a href="mailto:Paul.Halpin@eds.com">Paul.Halpin@eds.com</a>	(619) 817-3947
EDS Sherman Street Complex Visitor Request	EDS/NMCI Visitor Request 3970 Sherman Street San Diego, CA 92110	Security Office: (619) 817-3720 Fax: (619) 827-3715
Submit Navy Application Submission Packets to the NMCI PMO Precertification Lab	OTC – Receiving Officer N69255 SPAWAR Systems Center, San Diego ATTN: Ben Saville, 2833 4297 Pacific Highway, Building 7 San Diego, CA 92110	
Submit all Unclassified test applications and media	EDS Applications Lab 3970 Sherman Street San Diego, CA 92110 Attn: Albert Hatcher	
Submit all Classified test applications and media	Javier Berrellez (NMCI-ISF Security) NAVCOMTELSTA – NMCI NOC Attn: NMCI Security Room 246 Bldg. 1482 Read Rd. Naval Air Station North Island San Diego, CA 92135	
Questions/Concerns	<a href="mailto:mike.osnowitz@eds.com">mike.osnowitz@eds.com</a> <a href="mailto:steven.strull@eds.com">steven.strull@eds.com</a> <a href="mailto:paul.hapin@nmci-isf.com">paul.hapin@nmci-isf.com</a>	



Position/Billet	Email	Phone
	javier.berrellez@nmci-isf.com	
<b>Legacy Applications Liaison</b>		
Updates: <a href="https://tfw-opensource.spawar.navy.mil">https://tfw-opensource.spawar.navy.mil</a> (under contacts) <a href="http://www.nmci-isf.com/">http://www.nmci-isf.com/</a> .		
Navy	<a href="mailto:dslape@spawar.navy.mil">dslape@spawar.navy.mil</a>	(619) 524-4559
USMC	<a href="mailto:smbatnmci@mcsc.usmc.mil">smbatnmci@mcsc.usmc.mil</a>	(703) 784-3134

## Other

Topic	Email
Application Mapping Plan	<a href="mailto:NSCM_SCM@spawar.navy.mil">NSCM_SCM@spawar.navy.mil</a> <a href="mailto:smbatnmci@mcsc.usmc.mil">smbatnmci@mcsc.usmc.mil</a>
NMCI Help Desk Support	<a href="mailto:HelpDesk_NRFK@nmci-isf.com">HelpDesk_NRFK@nmci-isf.com</a>
NMCI RTD Prioritization and Scheduling (Unplanned Release)	<a href="mailto:nmci_scm@spawar.navy.mil">nmci_scm@spawar.navy.mil</a>
Quarantine Upgrade Emerging Support Team (QUEST)	<a href="mailto:NMCI_SCM@spawar.navy.mil">NMCI_SCM@spawar.navy.mil</a>
Request to Deploy	<a href="mailto:nmci_scm@spawar.navy.mil">nmci_scm@spawar.navy.mil</a>
Required Training	<a href="mailto:gary.smith-eds@eds.com">gary.smith-eds@eds.com</a>
Submission of Service Request Management (SRM) Distribution CLIN	<a href="mailto:mac@nmci-isf.com">mac@nmci-isf.com</a>
Submit RTD to NSCM/EBSS	<a href="mailto:nmci_scm@spawar.navy.mil">nmci_scm@spawar.navy.mil</a>

## APPENDIX D: NMCI APPLICATION RULESET (REVISED)

V2.96

NMCI Ruleset is also posted on NADTF website

[http://cno-n6.hq.navy.mil/navcio/leg\\_apps.htm](http://cno-n6.hq.navy.mil/navcio/leg_apps.htm)

Ruleset Is A Reference

The NMCI Ruleset is designed to be a summary of the information contained in the Legacy Applications Transition Guide (LATG) and the NMCI Release Development and Deployment Guide (NRDDG). Should questions arise from the use of the Ruleset, the user should refer to the LATG or NRDDG, or contact the Navy Applications Data Base Task Force (NADTF) for clarification.

Ruleset Number	Rule Name	Rule Description	Owner Required Action	Status
<b>RULE 1</b>	Windows 2000 (W2K) Compatible	The candidate application is not compatible with the Windows 2000 operating system. It either will not run properly under Windows 2000 or it will interfere with the normal functionality of the operating system.	Waivers will not be considered for this Ruleset. Claimant must resolve the incompatibility by working with the application POR/CDA and owning FAM to upgrade the application to Windows 2000 compatibility or it should be replaced by another that is Windows 2000 compliant. Once a compliant version is identified it will be submitted for NMCI testing and certification. Applications that cannot be corrected will be quarantined for no more than 6 months and then will be removed from the quarantine workstation. The application will then be removed from the rationalized list and archived in the ISF Tools Database. Echelon II commands will cancel the RFS and unlink the application from their UICs in the ISF Tools Database.	<b>FAIL</b>
<b>RULE 2</b>	NMCI Group Policy Object (GPO) Compatible	The candidate application is not compatible with the Group Policy Object (GPO) security rules for the workstation. For instance, if the candidate application requires full control of the c:\winnt folder in order to run, this violates NMCI enterprise policy governing connection to the NMCI network.	Waivers will not be considered for this Ruleset. Claimant must resolve the incompatibility by working with the application POR/CDA, owning FAM, ISF, and NMCI DAA to correct the GPO failure. NETWARCOM and ISF will provide the technical data detailing cause of the failure. Once the GPO failure is resolved, the application will be re-tested. GPO Policy changes may be requested from the NMCI DAA. Applications that cannot be corrected will be quarantined for no more than 6 months and then be removed from the quarantine workstation. If the application cannot be corrected, it must be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	<b>FAIL</b>

Ruleset Number	Rule Name	Rule Description	Owner Required Action	Status
<b>RULE 3</b>	No Duplication of Gold Disk Software or Services	The candidate application or service duplicates the functionality of the NMCI Standard Seat Services ("Gold Disk") applications. (Example: Word 2000 replaces all versions of WordPerfect and other word processors. Windows Media Player, Real Player, and QuickTime replace all other audio/video players).	Claimant should discard the current application and use the application or service that exists on the Gold Disk. This application is not eligible for quarantine. Waiver requests may be submitted to the appropriate FAM through the DADMS Waiver Questionnaire, but approvals will only be given if Claimant can show degradation to the mission, and can show that they cannot afford to upgrade to authorized NMCI software or services. If the waiver is not approved or if no waiver is submitted, the application must be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database	<b>KILL UNLESS WAIVER AUTHORIZED</b>
<b>RULE 4</b>	Comply with DON/NMCI Boundary 1 and 2-Policies	The ISF and NMCI DAA have determined, through testing, that the candidate application is non-compliant with NMCI Boundary firewall policies (violation of B1/B2 Rulesets).	Claimant must resolve violation with the application POR/CDA, owning FAM, ISF, and NMCI DAA to determine how to correct the Boundary policy violation. Once the policy violation is resolved, the application will be re-tested. Waivers will not be considered for this Ruleset. Requests to operate a non-compliant system for B1 Firewall policy violations are managed by OPNAV and B2 policy changes are reviewed and managed by the NMCI DAA. B2 boundary issues may be resolved by moving servers into NMCI enclave. Applications that cannot be corrected will be quarantined for no more than 6 months and will then be removed from the quarantine workstation. These applications will then be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	<b>FAIL</b>
<b>RULE 5</b>	No Setup, Installation, Deinstall, Update and Auto update Tools or Utilities	The candidate application is actually a tool or utility used to load and remove applications. Since ISF conducts all application installation and removal in NMCI, these types of files will not be authorized in ISF Tools DB or on the Rationalized List. Examples include Setup, Install, Uninstall, Launch, Auto launch, Run, Auto Run, Updater, Auto Updater or other installation-type Applications.	ISF will not test this application and waivers will not be considered. These types of applications will be removed from tracking and the Legacy Applications Rationalized List and archived in the ISF Tools database. It will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	<b>KILL</b>

Ruleset Number	Rule Name	Rule Description	Owner Required Action	Status
<b>RULE 6</b>	No Games	The candidate application is a "game" as defined by PEO-IT, NAVY IO and the PMO, and is prohibited on the NMCI environment.	ISF will not test this application unless the POR/CDA, Echelon II and/or FAM determine the game is required for mission accomplishment (Modeling, Simulation, or Training). The Claimant must submit a waiver request to the appropriate FAM through the DADMS Waiver Questionnaire. Applications already approved by the M&S and/or Training FAM will not require waivers. If the waiver is not approved or if no waiver is submitted, the application must be removed from the Legacy Applications Rationalized List and archived in the ISF Tools database. It will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	<b>KILL UNLESS WAIVER AUTHORIZED</b>
<b>RULE 7</b>	Restrictions on Freeware or Shareware	The candidate application is "Freeware" or "Shareware" as defined by PEO-IT, NAVY IO or the PMO, and significant restrictions are imposed for applications using shareware or freeware in the NMCI environment. Enterprise life cycle support and licensing issues accompany most "Freeware and Shareware" and are the responsibility of the CDA or sponsoring FAM.	The candidate application either employs "freeware and/or shareware" in the construct of a GOTS application or is a "freeware and/or shareware" application which is sponsored by a CDA or a FAM. Enterprise life cycle support and licensing must be provided by the responsible CDA or the responsible FAM prior to the submission of freeware/shareware for NMCI testing. Waivers for freeware and shareware must be submitted by the POR/CDA or FAM and be approved by the NADTF prior to NMCI testing using the DADMS Waiver Questionnaire. The waiver request must include the CDAs/FAMs commitment for enterprise lifecycle and licensing support. The NADTF will coordinate the waiver request with the NMCI DAA. Freeware/shareware applications will not be installed on quarantine networks and/or dual desktop configurations. If the waiver is not approved or if no waiver is submitted, the application must be removed from the Legacy Applications Rationalized List and archived in the ISF Tools database. The Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	<b>KILL UNLESS WAIVER AUTHORIZED</b>
<b>RULE 8</b>	No Beta/Test Software (Authorized on S&T Seats Only)	The candidate application is a "beta" or a "test" version, as defined by the PEO-IT, NAVY IO, or the PMO, and is therefore prohibited in the NMCI environment.	ISF will not test this application and a waiver will not be considered. These types of applications will not be tracked through the Legacy Application Transition process. These applications are not entered into the ISF Tools Database and not included on any rationalized list, nor should an RFS be submitted. If the Beta or Test Software is critical for mission accomplishment, the Claimant may purchase an S&T Seat. This application will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	<b>KILL</b>

Ruleset Number	Rule Name	Rule Description	Owner Required Action	Status
<b>RULE 9</b>	No Application Development Software (Authorized on S&T Seats Only)	The candidate application is "application development" software, as defined by either PEO-IT, NAVY IO or the PMO, and therefore is not authorized on standard NMCI Seats. The candidate application would be permitted if operated on an NMCI ordered Science and Technology (S&T) Seat. Application Development Software will not be tracked on the Rationalized List in the ISF Tools Database nor submitted for certification.	ISF will not test this application and a waiver will not be considered. These types of applications will not be tracked through the Legacy Application Transition process. These applications are not entered into the ISF Tools Database and not included on any rationalized list, nor should an RFS be submitted. If the application development software is critical for mission accomplishment, the Claimant may purchase an S&T Seat, which allows for the installation of development software. This application will not be installed on a quarantine workstation. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	<b>KILL</b>
<b>RULE 10</b>	No Agent Software	The candidate application is "agent" software, as defined by PEO-IT, NAVY IO or the PMO. Agents in the NMCI environment are controlled by ISF. No other candidate agents are allowed in the NMCI environment. Agents are code modules installed on client machines (or network devices) often used to poll, monitor, and collect system or network node performance data and send it to management consoles elsewhere on the network. These present a security risk to NMCI. Network monitoring and management are the responsibilities of the ISF.	These types of applications will be removed from tracking in the Legacy Applications Rationalized List and the ISF Tools Database. These applications will not be considered for waivers. No polling and monitoring of legacy networks and systems and collecting of data is authorized from within NMCI Polling, monitoring and collecting system and network data from legacy networks and systems is still authorized from legacy network assets only. Viewing collected legacy network or system data from NMCI seats is allowed using non-agent software.	<b>KILL</b>
<b>RULE 11</b>	Gold Disk Compatible	The application software is not compatible with the standard "Gold Disk" software and services. This means that the candidate application does not interact properly with one or more of the set of applications or services that have been selected to be installed on all NMCI seats.	Waivers will not be considered for this Ruleset. The application is quarantined for no more than 6 months and then it is removed from the quarantine workstation. The application will be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel the RFS and unlink this application from their UICs in the ISF Tools database. Claimants and POR/CDA must work with the ISF to determine Gold Disk compatibility issues. The POR/CDA then works with the owning FAM to upgrade, replace, or retire the	<b>FAIL</b>

Ruleset Number	Rule Name	Rule Description	Owner Required Action	Status
			application. Once a compliant version is identified it must be submitted for NMCI testing.	
<b>RULE 12</b>	No Peripherals, Peripheral Drivers or Internal Hardware	The candidate submission is a component (driver or hardware helper app) dealing directly with allowing a peripheral piece of hardware to function (Scanner, Printer, Plotters, Chartmakers, CDRW drive, ZIP or JAZ drive, Camcorder, PDA, etc). This enabling software must be tracked with the hardware on the Peripherals list and not entered into ISF Tools Database or listed on the Rationalized List. Internal hardware and the associated driver are not permitted within NMCI.	Peripherals and enabling software (drivers) are not entered into the ISF Tools Database nor placed on the Rationalized List. Peripherals and Peripheral Drivers are tracked separately from the ISF Tools Database and the Rationalized List, and are included in the Peripheral Drivers List. The Peripheral Drivers List is submitted to the ISF on-site for processing.  If the driver is part of a bundled software package, that bundled package is handled like an application. The bundled package is entered into the ISF Tools Database, placed on the Rationalized List, and tested by the ISF.	<b>KILL</b>
<b>RULE 13</b>	No personal, non-mission, or non-business related software	The candidate application is “personal, non-mission, or non-business related”, and is therefore prohibited in the NMCI environment.	ISF will not test this application unless the POR/CDA, Echelon II and/or FAM determine that this application is required for mission accomplishment. These applications will not be installed on a quarantine workstation. The claimant must submit a waiver request to the appropriate FAM through the DADMS Waiver Questionnaire. If the waiver is not approved or submitted, the application must be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	<b>KILL UNLESS WAIVER AUTHORIZED</b>

Ruleset Number	Rule Name	Rule Description	Owner Required Action	Status
<b>RULE 14</b>	8/16-Bit Applications	8-bit and 16-bit applications may migrate into the NMCI environment with an approved FAM waiver and a realistic migration plan that identifies a path to 32-bit status. Applications without approved waivers will not migrate to NMCI or Quarantined environments. Identification of an application as 8-bit or 16-bit does not stop the testing process (PIAB and LADRA). The application must pass all other rules and testing for 8-bit and 16-bit waivers to be approved.	Claimant and/or POR/CDA will submit a waiver immediately to the appropriate FAM through the DADMS Waiver Questionnaire requesting the 8/16-bit application migrate into NMCI. The request must include a detailed migration plan to get 8/16-bit application to 32-bit or web application status. ISF must process and certify the application while the waiver is being submitted. ISF will deploy the application while the waiver is being processed. If the waiver is not authorized (disapproved), the application is quarantined for no more than 6 months, then removed from the quarantine workstation and archived in the ISF Tools database. Applications for which a waiver was not submitted will not be quarantined, and will be removed from the rationalized list and archived in the ISF Tools database. Echelon II commands will cancel RFS and unlink this application from their UICs in the ISF Tools database.	<b>PROCESS AND CERTIFY APPLICATION DEPLOYMENT WHILE WAIVER IS AUTHORIZED</b>



<b>Definition</b>	
Fail	Fail is defined as violating the NMCI Application Ruleset by failing to successfully meet compliance or usability testing standards. These applications are flagged as Quarantined and will operate on a quarantined workstation in the legacy environment until the Ruleset violation or test failure is resolved or a waiver to operate within NMCI has been submitted and approved.
Kill	Kill is defined as violating the NMCI Application Ruleset. The application is not compliant with the rules and standards for applications within NMCI as set by the Navy IO. These applications will not be flagged as Quarantined and will be removed from the Rationalization List and ISF Tools database, unless a waiver to the rule is submitted and approved.
Application Development Software	Any software that generates or allows the user to create programming code which compiles into executable (.exe) files that are installed and can be run from the user's workstation. Application Development Software is only permitted to reside on S&T seats.
Agent Software	Any software that polls, monitors and/or captures network traffic or queries network nodes for the purpose of reporting the captured information back to the user or another network node. This type of information is considered sensitive and its capture and dissemination poses a security risk.

## APPENDIX E: FACTORS AND ISSUES FOR APPLICATION MIGRATION

This appendix presents baseline factors and potential issues for applications migrating to the NMCI environment.

Factor	Issue
1. The NMCI user desktop is Windows 2000.	<ul style="list-style-type: none"> <li>Are desktop applications Windows 2000-compliant?</li> </ul>
2. The NMCI desktop will be implementing Office 2000.	<ul style="list-style-type: none"> <li>Are there any interfaces to Office applications (Word, Excel) that might be affected by the Office 2000 implementation?</li> </ul>
3. User desktops have dynamic TCP/IP addresses.	<ul style="list-style-type: none"> <li>Are there any issues with changing TCP/IP addresses at the desktop?</li> </ul>
4. Servers moving into the NMCI network will have a different TCP/IP address assigned.	<ul style="list-style-type: none"> <li>Is there any hard coded logic based on TCP/IP addresses?</li> <li>Is there hard code in script files, configuration files, parameters, and database entries?</li> <li>Do external systems reference your server by TCP/IP address?</li> </ul>
5. Printers within the NMCI network have a different naming scheme than currently used.	<ul style="list-style-type: none"> <li>Are there any hard coded printer names embedded in the application or application scripts?</li> <li>Are there any unique desktop printing requirements (e.g., color, duplex, high speed, plotter, scanners, etc.)?</li> </ul>
6. An NMCI user logs on to NMCI with a user ID that is different from the current user ID structure. For single sign-on NT domains, it may be more reasonable at this time (until the majority of users are transitioned) to prompt the user for the ID and password rather than creating a pass through security mechanism.	<ul style="list-style-type: none"> <li>Are there hard coded tables that reference user IDs?</li> <li>Are database permissions by user ID?</li> <li>Are external interfaces sensitive to user ID?</li> </ul>

Factor	Issue
7. NMCI users will be dialing into the NMCI dial-up servers. The TCP/IP address from the NMCI dial-up is different from that currently used.	<ul style="list-style-type: none"> <li>• Do any issues relate to using a different dial-up facility than is currently in use?</li> <li>• Is anyone using PC/Anywhere or similar products?</li> </ul>
8. A standard software configuration product locks the NMCI desktop down.	<ul style="list-style-type: none"> <li>• Does the application install anything on the desktop?</li> <li>• Does the application install and uninstall properly in the Add/Remove program?</li> </ul>
9. Is your application in compliance with the Navy Marine Corps Firewall Baseline Configuration?	
10. Is all the desktop software available and configurable for standard software distribution?	
11. If this application runs under an emulator, are there any anticipated issues (keyboard mapping) when the standard NMCI emulator (Reflections) is used?	

Factor	Issue
12. Are there any other applications that interface with your application under NMCI?	<ul style="list-style-type: none"> <li>• Does your application update any data used by another application?</li> <li>• Does your application run upstream or downstream from another application that it might effect?</li> <li>• Does your application share files, access shared files, or use drive mappings across workstations or servers?</li> <li>• Does the application depend on portable browser-initiated code? JavaScript and Java Applets are supported in the NMCI environment, but ActiveX components are not. Active X components used on the browser (client) for application access by users outside NMCI will not be allowed by the NMCI boundary.</li> <li>• Does the application rely on desktop plug-ins?</li> <li>• Does the application need any supporting applications (such as web browsers, ORACLE, PowerBuilder, 4th Dimension, runtimes)?</li> </ul>
13. Does your application encrypt data during transmission or for storage? Does your application use encrypted data for input?	
14. Users do not have administrative rights to their local machines.	<ul style="list-style-type: none"> <li>• Developers must test applications with an account that does not have administrative rights.</li> </ul>
15. The NMCI gold disk includes common desktop applications.	<ul style="list-style-type: none"> <li>• As these applications may change over time, developers should develop to standard protocols and avoid the use of proprietary APIs.</li> </ul>

## APPENDIX F: DEVELOPER CHECKLIST

1. NMCI Release Management Process (NRMP)		
<b>1.1. Requirement</b>		
Requirement	Reference	Remarks
<input type="checkbox"/> Validate and document release system requirements.	NRDDG Paragraph 3.1.1	
<input type="checkbox"/> Review the restrictions NMCI places on release development and deployment (NMCI Application Ruleset and development policies).	NRDDG Paragraph 3.2 and Appendix D	
<input type="checkbox"/> Review all applicable NMCI CLINs.	NRDDG Paragraphs 4.11.1 and 4.12	
<input type="checkbox"/> Review NMCI-ISF website.		<a href="http://www.nmci-isf.com/">http://www.nmci-isf.com/</a>
<b>1.2. Approval</b>		
Requirement	Reference	Remarks
<input type="checkbox"/> Enter release information into DADMS.	NRDDG Paragraph 4.4, FAM Mid-Term Rationalization Guide v7.7	<a href="https://www.dadms.navy.mil">https://www.dadms.navy.mil</a>
<input type="checkbox"/> Complete and submit DADMS questionnaire.	NRDDG Paragraph 4.4, FAM Mid-Term Rationalization Guide v7.7	<a href="https://www.dadms.navy.mil">https://www.dadms.navy.mil</a>
<input type="checkbox"/> Obtain FAM approval to develop.	NRDDG Paragraph 3.1.2	<a href="https://www.dadms.navy.mil">https://www.dadms.navy.mil</a>
<b>1.3. Develop the Release</b>		
Requirement	Reference	Remarks
<input type="checkbox"/> Obtain and review NMCI release development policies, rules and requirements	NRDDG Paragraph 6.1.and Appendix G	
<input type="checkbox"/> Acquire an NMCI development environment to develop and test the release.	NRDDG Paragraph 6.2	CLIN 0038
<b>1.4. Request to Deploy Process</b>		
Requirement	Reference	Remarks
<input type="checkbox"/> Planned Release: Will release be ready to deploy within next 3 quarters?	NRDDG Paragraph 6.2	
<input type="checkbox"/> Unplanned Release: Is release being submitted as Emergency / Urgent release?	NRDDG Paragraph 6.2.2.2	
<input type="checkbox"/> Complete Request to Deploy (RTD) form for the release.	NRDDG Paragraph 6.3.1.2	
<input type="checkbox"/> Command review and approval.	NRDDG Paragraph 6.3.1.3	

<input type="checkbox"/> Submit the RTD w/Command endorsement to the NNWC/HQMC (C4)/EBSS.	NRDDG Paragraph 6.3.1.7	Navy: <a href="mailto:nmci_scm@spawar.navy.mil">nmci_scm@spawar.navy.mil</a> Marine Corps: <a href="mailto:smbatnmci@mcsc.usmc.mil">smbatnmci@mcsc.usmc.mil</a>
<b>2. NMCI Release Deployment Process (NRDP)</b>		
<b>2.1 Preparation</b>		
Requirement	Reference	Remarks
<input type="checkbox"/> Begin development of New or Updated DITSCAP documentation.	NRDDG Paragraph 4.7	DoD Inst 5200.40 DON IA Pub 5239.13 (Volumes I and II) DoD Instruction 8510.1-M <a href="http://iase.disa.mil/ditscap/index.html">http://iase.disa.mil/ditscap/index.html</a>
<b>2.1.1 Precertification</b>		
<input type="checkbox"/> Gather existing Precertification data, IATO/ATO/DITSCAP, SSAA documentation.	NRDDG Paragraph 6.5.5	Information required to meet Preparation requirement.
<input type="checkbox"/> Review and ensure software license requirements are met.	NRDDG Paragraph 6.5.5.1	Information used in Collection and Submission process.
<b>2.2 Collection and Submission</b>		
Requirement	Reference	Remarks
<input type="checkbox"/> Complete CDA RFS/USMC RFS.	NRDDG Paragraph 6.6.1	Use ISF Tools Database. Enter CDA RFS/USMC RFS # in the RDP. <a href="http://www.nmci-isf.com/transition.htm#Legacy">http://www.nmci-isf.com/transition.htm#Legacy</a>
<input type="checkbox"/> Create Application Submission Packet. <input type="checkbox"/> Release Media <input type="checkbox"/> Dependent or Supplemental Media <input type="checkbox"/> Copy of software license <input type="checkbox"/> Installation Instructions	NRDDG Paragraph 6.6.2 through 6.6.2.4	All Application Submission Packet items should be burned to CD (1 or more maybe required based on size of packet) and submitted via traceable means to the EDS Applications Lab, San Diego on or before the assigned submission date. Keep a copy on file for future use as required.
<input type="checkbox"/> Finalize and submit New or Updated DITSCAP documentation.	NRDDG Paragraphs 4.7 and 6.6.4	DITSCAP documentation is submitted to the Navy NMCI PMO NSCM or to the Marine Corps MCSC/for review and submission to the appropriate service NMCI DAA.
<input type="checkbox"/> Submit final Application Mapping to NSCM no later than 15 days before Required Deployment Date (RDD)	NRDDG Paragraph 6.6.3.6	<a href="mailto:Nmci_scm@spawar.navy.mil">Nmci_scm@spawar.navy.mil</a>
<b>2.3 Packaging and Certification</b>		
Requirement	Reference	Remarks
<input type="checkbox"/> Submit site visit request.	NRDDG Paragraph 6.7.3, Appendix I5 & I6	If the Developer plans on participating in Lab and Usability Test at the Applications Lab or CAL.

		Appendix I5 and I6
<input type="checkbox"/> Support for Quick Fix activity.	NRDDG Paragraph 6.7.5	
<b>2.4 Accreditation &amp; Risk Mitigation</b>		
<b>Requirement</b>	<b>Reference</b>	<b>Remarks</b>
<input type="checkbox"/> Disapproval - Conduct rework to mitigate unacceptable risk	NRDDG Paragraph 6.8	
<input type="checkbox"/> Approval - Submit NMCI DAA release ATO or IATO.	NRDDG Paragraph 6.8	
<b>2.5 Enterprise Change Control Board (ECCB)</b>		
<b>Requirement</b>	<b>Reference</b>	<b>Remarks</b>
<input type="checkbox"/> Support rework of Submission Packet to resolve issues raised by ECCB.	NRDDG Paragraph 6.10	

## **APPENDIX G:    RELEASE DEPLOYMENT PLAN (RDP)**

This appendix provides the RDP Form and Instruction Guide.

G1.	Release Deployment Plan Form .....	G-1
G2.	Release Deployment Plan Instruction Guide .....	G-1



## G1. Release Deployment Plan Form

<b>SECTION 1 – APPLICATION INFORMATION</b>			
Application Full Name:			
Acronym:	Version:		
CDA RFS number:	RTD number:		

<b>SECTION 2 – APPLICATION DEPLOYMENT/IMPLEMENTATION INFORMATION</b>			
<p>Application Developers shall ensure that specific information about the deployment of the release is provided. This information includes the synchronization of upgrades to server applications supporting a client release or a requirement to perform an incremental deployment of a release. The Application Developer will coordinate with the CCS to ensure these actions are scheduled and implemented into the deployment plan. Application Developer/POR-PM/Command must provide a listing of all sites that will be affected by the release.</p>			
<b>Communication and Key Correspondence Plan</b>			
Use this section to indicate any POCs that the Application Developer indicates will require notification during the process.			
Subject	POC	Email	Deployment Instructions
Media Submission			
Testing			
Pilot Test			
<b>Training Plan</b>			
Is this deployment dependent on a training plan? Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>			
If yes, please explain:			
Will the Implementation Team need training? Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>			
If yes, provide a training plan summary, and if necessary attach POA&M:			
<b>Implementation Plan</b>			
How many sites will be affected by this release? 0			
Is this deployment in conjunction with a server update or connection change?			
Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>			
If yes, describe server plan and attach server deployment schedule			
How is the application/release being deployed?			
Single Site <input type="checkbox"/>			
Region <input type="checkbox"/>			
Enterprise <input type="checkbox"/>			
Specialty COI (e.g. NNPI) <input type="checkbox"/> If specialty, identify the COI:			
Will existing hardware be upgraded or replaced?			
Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>			
If yes, please describe:			
Does the hardware have any special facilities requirements?			
(Electrical, A/C, racks, cable, fiber, etc.) Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/>			
If yes, please describe:			

<b>SECTION 2 – APPLICATION DEPLOYMENT/IMPLEMENTATION INFORMATION</b>																				
Do certificates and/or license keys need to be acquired to install this solution? Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> If yes, who will provide the certificates/license keys?																				
Will the solution impact other systems? Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> If yes, list systems <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr style="background-color: #d3d3d3;"> <th style="width: 30%;">System Name</th> <th style="width: 40%;">System Location</th> <th style="width: 30%;">Impact</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> </tbody> </table>			System Name	System Location	Impact															
System Name	System Location	Impact																		
Does the solution have to be deployed to multiple regions at the same time? Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> If yes, please explain:																				
Are there any special backup requirements prior to deployment? Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> If yes, please explain:																				
Are there any special site security requirements? Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> If yes, please explain:																				
Will the on-site resources need special authorization? Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> If yes, who will be obtaining this authorization?																				
Other than the standard NMCI Radia deployment, are there any other implementation requirements for this application: Yes <input type="checkbox"/> No <input type="checkbox"/> N/A <input type="checkbox"/> If yes, please provide a detail description																				
<b>Testing/Verification Plan</b>																				
During the deployment of the application, EDS conducts a series of test to help validate the deployment of the application. This testing/verification (ARDRA/Pilot Test) is conducted with a sample set or users. It is generally assumed that these users are aware of the testing process and can validate for the Application Developer the operational content of the application. To assist in preparing for this test, please complete the following questions.																				
Is there a test plan that can be used in verification of the client applications at deployment? Yes <input type="checkbox"/> No <input type="checkbox"/> If yes, please provide the test plan as an attachment. If no, please describe how the client can be verified?																				
Please identify a sample list of users for the ARDRA/Pilot Test. To ensure accuracy to the test, users should be selected from multiple regions and services where appropriate. <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr style="background-color: #d3d3d3;"> <th style="width: 35%;">User Name</th> <th style="width: 35%;">Email Address</th> <th style="width: 30%;">Phone Number</th> </tr> </thead> <tbody> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> <tr><td> </td><td> </td><td> </td></tr> </tbody> </table>			User Name	Email Address	Phone Number															
User Name	Email Address	Phone Number																		

## **G2. Release Deployment Plan Instruction Guide**

The Release Deployment Plan (RDP) documentation is necessary for a successful deployment of an application into the NMCI environment and an incomplete or an improperly completed RDP will directly impact the deployment of the application release. It is the responsibility of the Developer to develop the RDP and to ensure that the information is completed as timely and as accurately as possible. The Developer is encouraged to read and follow the detailed packaging, testing, certification, and deployment instructions contained in the NMCI Release Development and Deployment Guide (NRDDG).

### **RTD/RDP Process**

Integration of an application release into the NMCI environment requires the submission of the Request to Deploy (RTD) and the Release Deployment Plan (RDP) to [nmci\\_scm@spawar.navy.mil](mailto:nmci_scm@spawar.navy.mil) and the media submission to the test and certification lab.

The Application Mapping should be as complete as possible at the time that the RDP is submitted. Shortly after the media has been received by the test and certification lab, a report will be generated that will identify all seats using a previous version of this application. It is important to note that locally loaded applications may not appear on this report. The Developer is encouraged to review this report and submit any changes or modifications using the Application Mapping template. The Developer can request an electronic copy of the Application Mapping template from their CCS representatives or request a copy at [nmci\\_scm@spawar.navy.mil](mailto:nmci_scm@spawar.navy.mil)

### **RDP Due Date**

For Non-emergency deployments: The final application mapping must be submitted no later than 30 days after media submission.

For Emergency deployments: The final application mapping must be submitted no later than 15 days after media submission.

### **RDP Submission**

The completed RDP form is submitted electronically to [nmci\\_scm@spawar.navy.mil](mailto:nmci_scm@spawar.navy.mil) and as the application progresses through the deployment phase email notifications will be sent to the Developer, Alternate Point of Contact (POC), and Command in order to keep all concerned informed of the status of the application.

### **RDP Service Support**

If assistance is required for the completion of the RDP form, contact your assigned NSCM Claimant CDA Support (CCS) person or contact Service Support Monday through Friday during the hours of 0800 to 1600 (Pacific Time) (619) 524-4554 or through email to [nmci\\_scm@spawar.navy.mil](mailto:nmci_scm@spawar.navy.mil)

## Section 1 – Application Information

1. Application Full Name: Enter the full name of the release, this includes a new release or release that modifies, upgrades, or updates an existing application. It is important to ensure that the application name is the same on the RDP, RTD, in the ISF Tools Database, and in the DON Application & Database Management System (DADMS).
2. Acronym: Enter the abbreviated name of the application. It is important to ensure that the acronym name is the same on the RDP, RTD, in the ISF Tools Database, and in the DON Application & Database Management System (DADMS).
3. Version: Enter the version number of the application. It is important to ensure that the version name is the same on the RDP, RTD, in the ISF Tools Database, and in the DON Application & Database Management System (DADMS).
4. CDA RFS Number: The CDA RFS number is listed in the ISF Tools Database.
5. RTD Number: Enter the Request to Deploy (RTD) number

## SECTION 2 – APPLICATION DEPLOYMENT/IMPLEMENTATION INFORMATION

### Communication and Key Correspondence Plan

6. This information will be used to contact appropriate personnel for the synchronization of upgrades to server applications in support of a client release, incremental deployment instructions, and coordination of the scheduled deployment plan. Enter the point of contact name, email, and deployment instructions for Application Developer that will require notification during the deployment process.

### Training Plan

7. Is this deployment dependent on a training plan? Check yes, no, or non-applicable (N/A). If yes is select, explain what type of training and when training will take place.
8. Will the Implementation Team need training? Check yes, no, or non-applicable (N/A). If yes is selected, provide a training plan summary and if necessary attach a Plan of Action & Milestone (POA&M).

### Implementation Plan

9. How many sites will be affected by this release? Enter the number of sites.
10. Is this deployment in conjunction with a server update or connection change? Check yes, no, or non-applicable (N/A). If yes is selected, describe server update plan and attach the server deployment schedule, if necessary (POA&M).
11. How is the application/release being deployed? Single Site, Region, Enterprise, Specialty COI (NNPI). If specialty, identify the CPO/NNPI
12. Will the existing hardware be upgraded or replaced? Check yes, no, or non-applicable (N/A). If yes is selected, please describe

13. Does the hardware have any special facilities requirements? Check yes, no, or non-applicable (N/A). If yes is selected, describe electrical, a/c, racks, cable, fiber, etc).
14. Do certificates/license keys need to be acquired to install this solution? Check yes, no, or non-applicable (N/A). If yes is selected, who will provide the certificates/license keys?
15. Will the solution impact other systems? Check yes, no, or non-applicable (N/A). If yes is selected, list the system name, system location, and the impact to the system.
16. Does the solution have to be deployed to multiple regions at the same time? Check yes, no, or non-applicable (N/A). If yes is selected please explain.
17. Are there any special backup requirements? Check yes, no, or non-applicable (N/A). If yes is selected, please explain.
18. Are there any special site requirements? Check yes, no, or non-applicable (N/A). If yes is selected, please explain.
19. Will the on-site resources need special authorization? Check yes, no, or non-applicable (N/A). If yes is selected, who will be obtaining this authorization?
20. Other than the standard NMCI Radia deployment, are there any other implementation requirements for this application? Check yes, no, or non-applicable (N/A). If yes is selected, please provide a detail description.
21. Is there test plan that can be used in verification of the client applications at deployment? Check yes, or no. If yes is selected, please provide the test plan as an attachment. If no is selected, describe how the client can be verified.
22. Identify a sample list of users for the ARDRA/Pilot Test. To ensure accuracy to the test, users should be selected from multiple regions and services where appropriate. Provide user name, email address, and phone number.

*Include electronic copy of the Application Mapping for User to Application Mapping or Machine Mapping information with the electronic copy of the RDP and submit to [nmci\\_scm@spawar.navy.mil](mailto:nmci_scm@spawar.navy.mil). Requests for electronic copy of the mapping templates can be made at the same email address.*

## APPENDIX H: NAVY FUNCTIONAL AREA MANAGER (FAM) LIST

Functional Area	Responsible Organization (Navy)	Responsible Organization (USMC)	Key Secretariate Stakeholder
Acquisition	ASN (RD&A)		
Financial Management	ASN (FM&C)		
Civilian Personnel	ASN (M&RA)		
Legal	GC/JAG		
Administration	DNS	HQMC AR	AAUSN
Manpower and Personnel	OPNAV N1	HQMC M&RA	ASN (M&RA)
Intelligence & Cryptology	OPNAV N2	HQMC I	ASN (R&D)
Logistics (Includes Facilities Mgt & Environment)	OPNAV N4	HQMC I&L	ASN (I&E) ASN (RD&A)
Readiness	OPNAV N4	HQMC PP&O	ASN (RD&A)
Command, Control and Communications	OPNAV N6/N7	HQMC C4	ASN (RD&A)
Information Warfare	OPNAV N6/N7	HQMC PP&O	ASN (RD&A)
Modeling & Simulation	OPNAV N6/N7	MCSC SE&I	ASN (RD&A)
Weapons Planning and Control	OPNAV NOON	HQMC	ASN (RD&A)
Training and Education	OPNAV N79	TECOM	ASN (M&RA)
Resources, Requirements and Assessments	OPNAV N8	HQMC P&R	ASN (FM&C)
Scientific & Technical	OPNAV N091	MCCDC	ASN (RD&A)
Test & Evaluation	OPNAV N091	MCOTEA	ASN (RD&A)
Medical	OPNAV N093		
Reserve Affairs	OPNAV N095	HQMC M&RA	ASN (MR&A)
Meteorology, Oceanography, GI&S	OPNAV 096		ASN (RD&A)
Precise Time and Astrometry	OPNAV 096		ASN (RD&A)
Religious Ministries	OPNAV N097		
Naval Nuclear Propulsion	OPNAV NOON		

## **APPENDIX I:     EXAMPLES AND TEMPLATES**

This appendix provides examples and templates for use by developers as part of documenting, developing, and deploying releases.

I1.	Example Test Script.....	I-2
I2.	Example Installation Instruction.....	I-8
I3.	Example Application Mapping Template.....	I-12
I4.	Example of Systems Architecture Connectivity Diagram.....	I-13
I5.	EDS Sherman Street Complex Visitor Request.....	I-16
I6.	ARDRA/Pilot Test.....	I-17

## **I1. Example Test Script**

### **Sample Test Script**

This is an example of test cases and procedures used by EDS to test the proper installation and functionality of the software.

### **Generating SQL Scripts for SMS Views**

The information in this article applies to:

- Microsoft Systems Management Server 1.1
- Microsoft Systems Management Server 1.2

This article was previously published under Q133253.

### **Summary**

SMSVIEW creates various views that can be used when querying the Systems Management Server SQL Database. The SQL Scripts used to create these views can be dumped using Microsoft SQL Enterprise Manager (in Microsoft SQL Server 6.0).

### **More Information**

To generate the SQL scripts to create the SMS views:

1. Start SQL Enterprise Manager.
2. If the server where the Systems Management Server database resides is not already registered in SQL Enterprise Manager, register it as follows:
  1. Select Register Server from the Server menu.
  2. Provide the server name and valid logon information (by default, the valid logon is SA with no password and Standard Security).
  3. Choose Register.
3. In the Server Manager window, select the server you just registered (there may be a slight delay as a connection to this server is established).
4. Choose + in the following order:
  1. The Server's name in the Server Manager window.
  2. Databases to get to the Systems Management Server database.
  3. The database that contains the Systems Management Server data.



The name of the SMS database in the Server Manager window should be selected.

5. Select Generate SQL Scripts from the Object menu.
6. In the Generate SQL Scripts - <servername>\<database name> dialog box, choose All Views for Scripting Objects. This fills in the name of each view in the list box at the bottom right portion of the dialog box.
7. Ensure Object Creation and Object Drop are selected for Scripting Options.
8. If you prefer scripts for each view to be placed in a separate file, select Per Object in Scripting Options. Otherwise, select Single File.
9. Choose Preview (there is a short wait as the scripts are generated). Save the scripts as text files or choose Close to go back to the Generate SQL Scripts dialog box without saving the scripts).

The following displays the resulting output (in Systems Management Server 1.1, Build 682):

```
/***** Object: View dbo.vDisk   Script Date: 7/5/95 4:30:43 AM *****/
if exists (select * from sysobjects where id = object_id('dbo.vDisk') and
sysstat & 0xf = 2)
drop view dbo.vDisk
GO
Create View vDisk as select dwMachineID , Disk_SPEC.__Disk_Full0 ,
Disk_COMM.Disk_Index0 , Disk_COMM.File_System0 ,
Disk_SPEC.Free_Storage__MByte_0 , Disk_SPEC.Sectors0 ,
Disk_SPEC.Serial_Number0 , Disk_SPEC.Storage_Size__MByte_0 ,
Disk_COMM.Storage_Type0 , Disk_SPEC.Storage_Used__MByte_0 ,
Disk_SPEC.Volume_Name0 from MachineDataTable ,Disk_COMM , Disk_SPEC
where Disk_COMM.datakey =* CommonKey and Disk_SPEC.datakey =* SpecificKey
and ArchitectureKey = 5 and GroupKey = 8
GO
/***** Object: View dbo.vEnvironment   Script Date: 7/5/95 4:30:43 AM
*****/
if exists (select * from sysobjects where id =
object_id('dbo.vEnvironment')
and sysstat & 0xf = 2)
drop view dbo.vEnvironment
GO
Create View vEnvironment as select dwMachineID ,
Environment_SPEC.Environment_String0 , Environment_SPEC.Value0 from
MachineDataTable ,Environment_COMM , Environment_SPEC where
Environment_COMM.datakey =* CommonKey and Environment_SPEC.datakey =*
SpecificKey and ArchitectureKey = 5 and GroupKey = 12
GO
/***** Object: View dbo.vGroupNames   Script Date: 7/5/95 4:30:44 AM
*****/
if exists (select * from sysobjects where id = object_id('dbo.vGroupNames')
```

```
and sysstat & 0xf = 2)
drop view dbo.vGroupNames
GO

Create View vGroupNames as select GM.GroupName FROM ArchitectureMap AM,
GroupMap GM WHERE GM.ArchitectureKey = AM.ArchitectureKey AND
((AM.Mode=0))
GO

/***** Object: View dbo.vIdentification Script Date: 7/5/95 4:30:44 AM
*****/
if exists (select * from sysobjects where id =
object_id('dbo.vIdentification') and sysstat & 0xf = 2)
drop view dbo.vIdentification
GO
Create View vIdentification as select dwMachineID ,
Identification_SPEC.Domain0 , Identification_SPEC.LogOn_Name0 ,
Identification_SPEC.Name0 , Identification_SPEC.NetCardID0 ,
Identification_SPEC.Site0 , Identification_SPEC.SMSID0 ,
Identification_SPEC.SMSLocation0 , Identification_SPEC.SystemRole0 ,
Identification_SPEC.SystemType0 from MachineDataTable
,Identification_COMM
, Identification_SPEC where Identification_COMM.datakey =* CommonKey and
Identification_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 1
GO

/***** Object: View dbo.vMouse Script Date: 7/5/95 4:30:44 AM *****/
if exists (select * from sysobjects where id = object_id('dbo.vMouse') and
sysstat & 0xf = 2)
drop view dbo.vMouse
GO
Create View vMouse as select dwMachineID , Mouse_COMM.Hardware_Installed0 ,
Mouse_COMM.Language0 , Mouse_COMM.Manufacturer0 ,
Mouse_COMM.Mouse_Hardware_Type0 , Mouse_COMM.Number_of_Buttons0 from
MachineDataTable ,Mouse_COMM , Mouse_SPEC where Mouse_COMM.datakey =*
CommonKey and Mouse_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 4
GO

/***** Object: View dbo.vNetcard Script Date: 7/5/95 4:30:45 AM
*****/
if exists (select * from sysobjects where id = object_id('dbo.vNetcard')
and
sysstat & 0xf = 2) drop view dbo.vNetcard
GO
Create View vNetcard as select dwMachineID , Netcard_SPEC.IRQ0 ,
```

```
Netcard_COMM.Manufacturer0 , Netcard_SPEC.Port_Address0 from
MachineDataTable ,Netcard_COMM , Netcard_SPEC where Netcard_COMM.datakey
=* CommonKey and Netcard_SPEC.datakey =* SpecificKey and ArchitectureKey =
5 and GroupKey = 11
GO
/***** Object: View dbo.vNetwork   Script Date: 7/5/95 4:30:45 AM
*****/
if exists (select * from sysobjects where id = object_id('dbo.vNetwork')
and

sysstat & 0xf = 2) drop view dbo.vNetwork
GO
Create View vNetwork as select dwMachineID , Network_COMM.Default_Gateway0
,
Network_SPEC.IP_Address0 , Network_SPEC.IPX_Address0 ,
Network_COMM.LogOn_Name0 , Network_COMM.Major_Version0 ,
Network_COMM.Minor_Version0 , Network_SPEC.Network_Active0 ,
Network_COMM.Network_Type0 , Network_COMM.Subnet_Mask0 from
MachineDataTable ,Network_COMM , Network_SPEC where Network_COMM.datakey
=* CommonKey and Network_SPEC.datakey =* SpecificKey and ArchitectureKey =
5 and GroupKey = 10
GO

/***** Object: View dbo.vOperating_System   Script Date: 7/5/95 4:30:45
AM *****/
if exists (select * from sysobjects where id =
object_id('dbo.vOperating_System') and sysstat & 0xf = 2)
drop view dbo.vOperating_System
GO
Create View vOperating_System as select dwMachineID ,
Operating_System_COMM.Build_Number0 , Operating_System_COMM.Build_Type0 ,
Operating_System_COMM.Country_Code0 ,
Operating_System_SPEC.Installation_Date0 ,
Operating_System_COMM.Language_ID0 ,
Operating_System_COMM.Operating_System_Name0 ,
Operating_System_COMM.Registered_Organization0 ,
Operating_System_SPEC.Registered_Owner0 ,
Operating_System_SPEC.System_Root0
, Operating_System_SPEC.System_Start_Options0 ,
Operating_System_COMM.Version0 from MachineDataTable
,Operating_System_COMM , Operating_System_SPEC where
Operating_System_COMM.datakey =* CommonKey and
Operating_System_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 7
GO
```

```
/****** Object: View dbo.vPC_Memory   Script Date: 7/5/95 4:30:46 AM
*****/

if exists (select * from sysobjects where id = object_id('dbo.vPC_Memory')
and sysstat & 0xf = 2)
drop view dbo.vPC_Memory
GO

Create View vPC_Memory as select dwMachineID ,
PC_Memory_SPEC.Page_File_Name0 , PC_Memory_SPEC.Page_File_Size_MByte_0 ,
PC_Memory_SPEC.Total_Paging_File_Space_0 ,
PC_Memory_SPEC.Total_Physical_Memory_KB0 from MachineDataTable
,PC_Memory_COMM , PC_Memory_SPEC where PC_Memory_COMM.datakey =*
CommonKey and PC_Memory_SPEC.datakey =* SpecificKey and ArchitectureKey = 5
and GroupKey = 9
GO

/****** Object: View dbo.vProcessor   Script Date: 7/5/95 4:30:46 AM
*****/

if exists (select * from sysobjects where id = object_id('dbo.vProcessor')
and sysstat & 0xf = 2)
drop view dbo.vProcessor
GO

Create View vProcessor as select dwMachineID ,
Processor_COMM.Processor_Name0 , Processor_COMM.Processor_Type0 ,
Processor_COMM.Quantity0 from MachineDataTable ,Processor_COMM ,
Processor_SPEC where Processor_COMM.datakey =* CommonKey and
Processor_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 6
GO

/****** Object: View dbo.vServices   Script Date: 7/5/95 4:30:46 AM
*****/

if exists (select * from sysobjects where id = object_id('dbo.vServices')
and sysstat & 0xf = 2)
drop view dbo.vServices
GO

Create View vServices as select dwMachineID , Services_SPEC.EXE_Path0 ,
Services_COMM.Name0 , Services_SPEC.Start_Name0 , Services_COMM.Start_Type0
, Services_COMM.State0 from MachineDataTable ,Services_COMM ,
Services_SPEC where Services_COMM.datakey =* CommonKey and
Services_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and
GroupKey = 13
GO

/****** Object: View dbo.vVideo   Script Date: 7/5/95 4:30:47 AM *****/

if exists (select * from sysobjects where id = object_id('dbo.vVideo') and
sysstat & 0xf = 2)
drop view dbo.vVideo
GO

Create View vVideo as select dwMachineID , Video_COMM._nd_Adapter_Type0 ,
```

```
Video_COMM.Adapter_Type0 , Video_SPEC.Bios_Date0 ,
Video_COMM.Current_Video_Mode0 , Video_COMM.Display_Type0 ,
Video_COMM.Manufacturer0 , Video_COMM.Max_Rows0 from MachineDataTable
,Video_COMM , Video_SPEC where Video_COMM.datakey =* CommonKey and
Video_SPEC.datakey =* SpecificKey and ArchitectureKey = 5 and GroupKey = 5
GO

/***** Object: View dbo.vWorkstationStatus   Script Date: 7/5/95 4:30:47
AM *****/
if exists (select * from sysobjects where id =
object_id('dbo.vWorkstationStatus') and sysstat & 0xf = 2)
drop view dbo.vWorkstationStatus
GO

Create View vWorkstationStatus as select dwMachineID ,
WorkstationStatus.Failed_Hardware_Checks0 ,
WorkstationStatus.Files_Not_Installed0 , WorkstationStatus.LastHWScan ,
WorkstationStatus.LastSWScan , WorkstationStatus.Standalone_Workstation0 ,
WorkstationStatus.System_Files_Not_Modified0 from MachineDataTable ,
WorkstationStatus where WorkstationStatus.datakey =* SpecificKey and
ArchitectureKey = 5 and GroupKey = 2
GO
```

## **I2. Example Installation Instruction**

**The following is an example of an installation instruction that EDS will use to install the release for testing.**

---

Visio2000: Revised Network Installation Instructions (Network.wri) for  
Visio 2000 Standard Edition  
The information in this article applies to:  
Microsoft Visio 2000 Standard Edition  
This article was previously published under Q258467

### **Summary**

The Network.wri file that is included with Microsoft Visio 2000 Standard Edition contains incorrect instructions for how to perform a network installation.

This article contains the full text of the Network.wri file, with the corrections incorporated. Use the information in this article instead of the Network.wri file when you need to do either of the following:

- Install Visio 2000 Standard Edition to a network drive for shared use.
- Install Visio 2000 Standard Edition locally from a network drive.

### **More Information**

Visio® 2000 Standard Edition  
Network Installation Instructions  
Copyright© 1991 - 1999 Visio Corporation. All rights reserved.  
File version 6.0.0 Visio(R) 2000 Standard Edition US English version  
Network Installation Instructions  
This file contains information about setting up and running Visio 2000 on a network.  
We recommend that you read this file and keep a printed copy with your Visio documentation. For other late-breaking information about installing and running  
Visio 2000, see the README.WRI file. For a list of all the files copied to your hard drive if you install the complete version of Visio 2000, see the  
FILELIST.WRI file.

### **Contents**

1. Network Licensing Information
2. Operations System Requirements for VISIO 2000
3. Network Setup Overview
4. Preparing a Workstation to Set Up VISIO for Shared Use
5. Setting Up VISIO 2000 on a Network Server for Shared Use
6. Setting Up VISIO 2000 on a Network Server for Local Installation to Workstations
7. Defining Default File Paths for VISIO Files
8. Opening VISIO Files on a Network
9. Using Filters with VISIO in Shared Windows Environment

## **1. NETWORK LICENSING INFORMATION**

To run Visio on a network that gives more than one-person access to the product, you need to acquire additional licenses either by purchasing additional retail packages of Visio or by purchasing license packs.

A license pack, which authorizes one additional user, includes a product license, a serialized registration card, and a documentation order form.

## **2. OPERATING SYSTEM REQUIREMENTS FOR VISIO 2000**

To use Visio 2000 Standard Edition, you must be running one of the following 32-bit Microsoft Windows operating systems:

- Microsoft Windows 95
- Microsoft Windows 98
- Microsoft Windows NT 4.0 (Service Pack 3 or later is required)

Service Packs for Windows 95, Windows 98, and Windows NT operating systems can be obtained from Microsoft Corporation ([www.microsoft.com](http://www.microsoft.com)).

**NOTE:** To install Visio 2000 on a workstation running Windows NT 4.0, the user installing the product must have Administrator privileges for that workstation.

**NOTE:** Installation Path Length Limitation: To ensure operation of the Visio 2000 Solutions, the directory chosen for installation of Visio 2000 Standard Edition must have a path name of less than 55 characters in length.

## **3. NETWORK SETUP OVERVIEW**

Setting up Visio on a network is a two-step process: First, you install Visio on the network server; second, you set up individual workstations so they can run Visio from the server or from each workstation's hard disk.

**NOTE:** Setting up Visio 2000 on a network server for shared use requires Windows NT 4.0 SP 3 or later. This procedure is not supported under Windows 95 or Windows 98.

For details about setting up Visio on a network so that multiple workstations can use a shared copy from the server, see "SETTING UP VISIO 2000 ON A NETWORK SERVER FOR SHARED USE" below.

For details about setting up Visio files on a network server so that the program can be loaded onto the hard disks of individual workstations, see "SETTING UP VISIO 2000 ON A NETWORK SERVER FOR LOCAL INSTALLATION TO WORKSTATIONS" below.

## **4. PREPARING A WORKSTATION TO SET UP VISIO FOR SHARED USE**

The Visio 2000 setup program is based on the Microsoft Windows Installer (.msi) technology. .msi must be installed on the workstation you are using to set up Visio 2000 for shared use before starting the Visio 2000 setup program. If .msi is not installed on the workstation, or if you are in doubt, use the following procedure to install .msi:

1. Insert the Visio 2000 CD into your CD-ROM drive.
2. From the Start menu, choose Run.
3. Type d:\Install\bin\sp\MSI\WinNT\InstMSI, where d is the letter assigned to your CD-ROM drive.

After installing .msi, complete the following procedure to install Visio 2000.

## **5. SETTING UP VISIO 2000 ON A NETWORK SERVER FOR SHARED USE**

To install Visio 2000 on a network server for shared use:

You must have write access to the network server to install Visio on the server.

**NOTE:** Do not run the Setup.exe file located in the root directory of the Visio CD for this procedure. This file is for single-user installations only, and will not install Visio correctly for shared use.

1. From a workstation running Windows NT 4.0, log on to the network and connect to the drive where you want to install the Visio program.
2. Insert the Visio 2000 CD into your CD-ROM drive.
3. From the Start menu, choose Run.
4. Type d:\Install\Setup /a where d is the letter assigned to your CD-ROM drive. Setup prompts you for the location of your Visio installation.
5. Type e:\visio, where e is the letter assigned to the network server and Visio is the directory on the server where the Visio program files will reside.
6. Follow the instructions on your screen.

Setup /a installs the Visio program files and creates the following subdirectory: Visio\Bin, for Visio product files.

To set up a workstation to run Visio from a network server:

1. On the workstation, from the Start menu, choose Run.
2. Type e:\Visio\setup, where e is the drive letter and \Visio is the directory on the server where the Visio setup program resides.
3. Follow the instructions on the screen.

The workstation setup does the following:

- Installs or updates any Windows system and shared files required by Visio.
- Adds Visio 2000 to the Start Menu.

## **6. SETTING UP VISIO 2000 ON A NETWORK SERVER FOR LOCAL INSTALLATION TO WORKSTATIONS**

You can place Visio 2000 files on a network server by following the steps in the preceding section, "SETTING UP VISIO 2000 ON A NETWORK SERVER FOR

SHARED USE." Then, users can connect to the directory and run the Setup program to install Visio on their workstations.

To install Visio 2000 from a network server to a workstation:



1. On the workstation, from the Start menu, choose Run.
2. Type f:\visio\setup where f is the drive letter and Visio is the directory on the server where the Visio setup program resides.
3. Follow the instructions on the screen.
4. When Setup prompts you for an installation location, type c:\program files\Visio, where c is the letter assigned to the workstation hard drive and \program files\Visio is the directory on your workstation where the Visio program will reside.

## **7. DEFINING DEFAULT FILE PATHS FOR VISIO FILES**

Users can define default file paths for Visio drawings, templates, add-ons, and filters. To specify these custom paths, choose Options... from the Visio Tools menu, and then click the File Paths tab. File paths defined here are written into the user's registry under the

HKEY\_LOCAL\_MACHINE\Software\Visio\Visio 2000 key. Click the Help button on the File Paths tab for more information.

## **8. OPENING VISIO FILES ON A NETWORK**

Working with and opening Visio files on a network is essentially the same as on an individual workstation. On the network, however, you can make a drawing available to other users and allow them to make changes to the file. You can also protect the file from changes.

\* Keep the following issues in mind when using Visio on a network:

You can share stencil files so that multiple users can access them at once. However, when you share stencil files, it is important that users not open them in read/write mode. (When a Visio drawing file is opened in read/write mode, no other network user can access the file.)

By default, the read-only attribute is set for stencil files to prevent users from opening them in read/write mode. You can also set the network Visio directory to read-only to prevent users from opening the files in read/write mode.

## **9. USING FILTERS WITH VISIO IN SHARED WINDOWS ENVIRONMENTS**

If you are using Visio 2000 in a shared Windows environment in which system files are write-protected, Visio 2000 cannot store custom filter settings. You will need to make changes to any filter defaults each time you use that filter - changes will not be retained from one use to the next.

Visio 2000 Standard Edition

END of Network Installation Instructions

The application-mapping plan is critical to the successful deployment of applications to existing NMCI seats. Where possible, EDS will supply current mapping information to identify the status and location of previously deployed releases. It is the responsibility of the Application Developer/CTR to identify and approve the application mapping of each release prior to EDS initiating deployment.

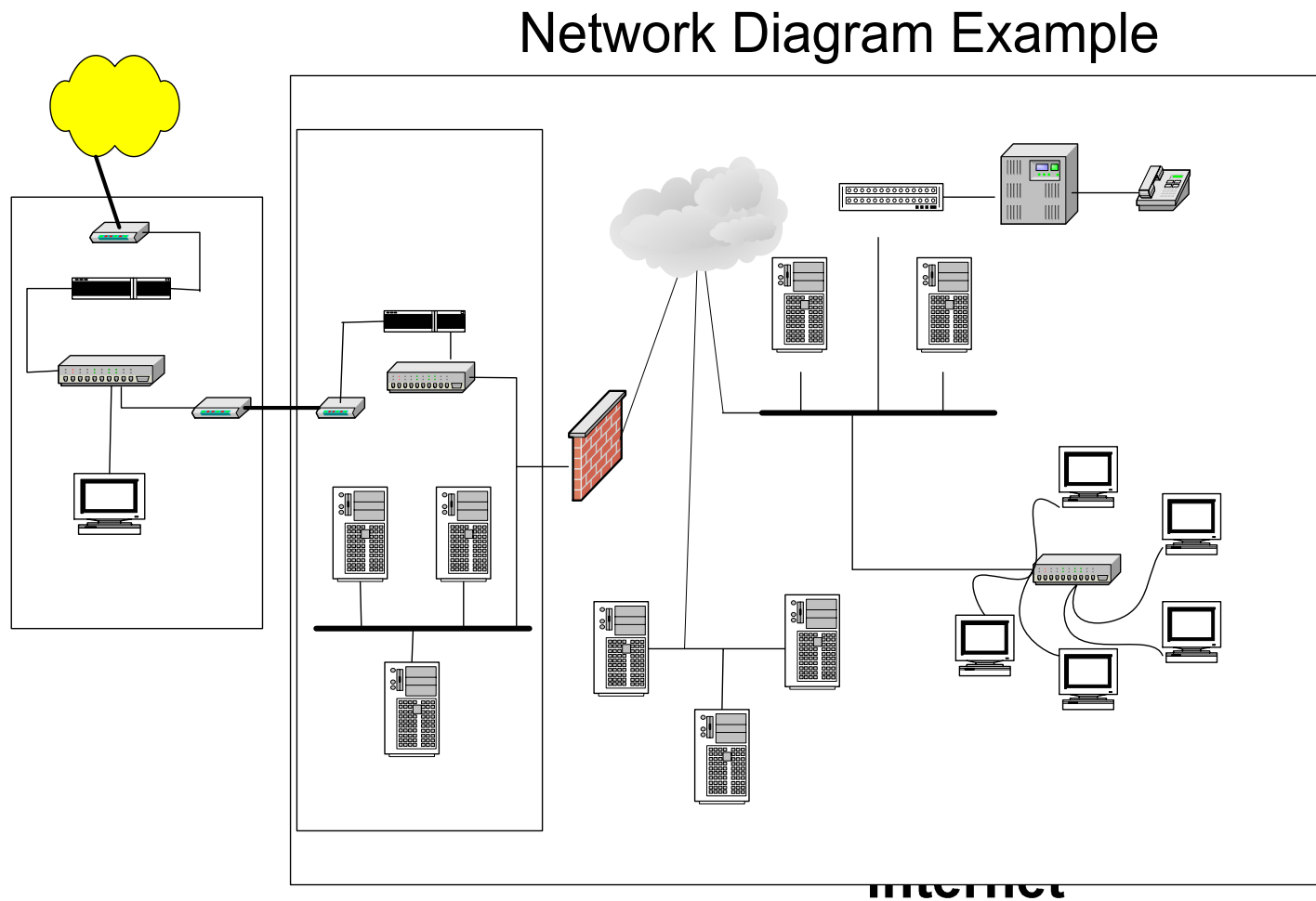
### QUEST Application Mapping (UTAM/STAM)

[illegible]

### QUEST Application Mapping (UTAM/STAM)

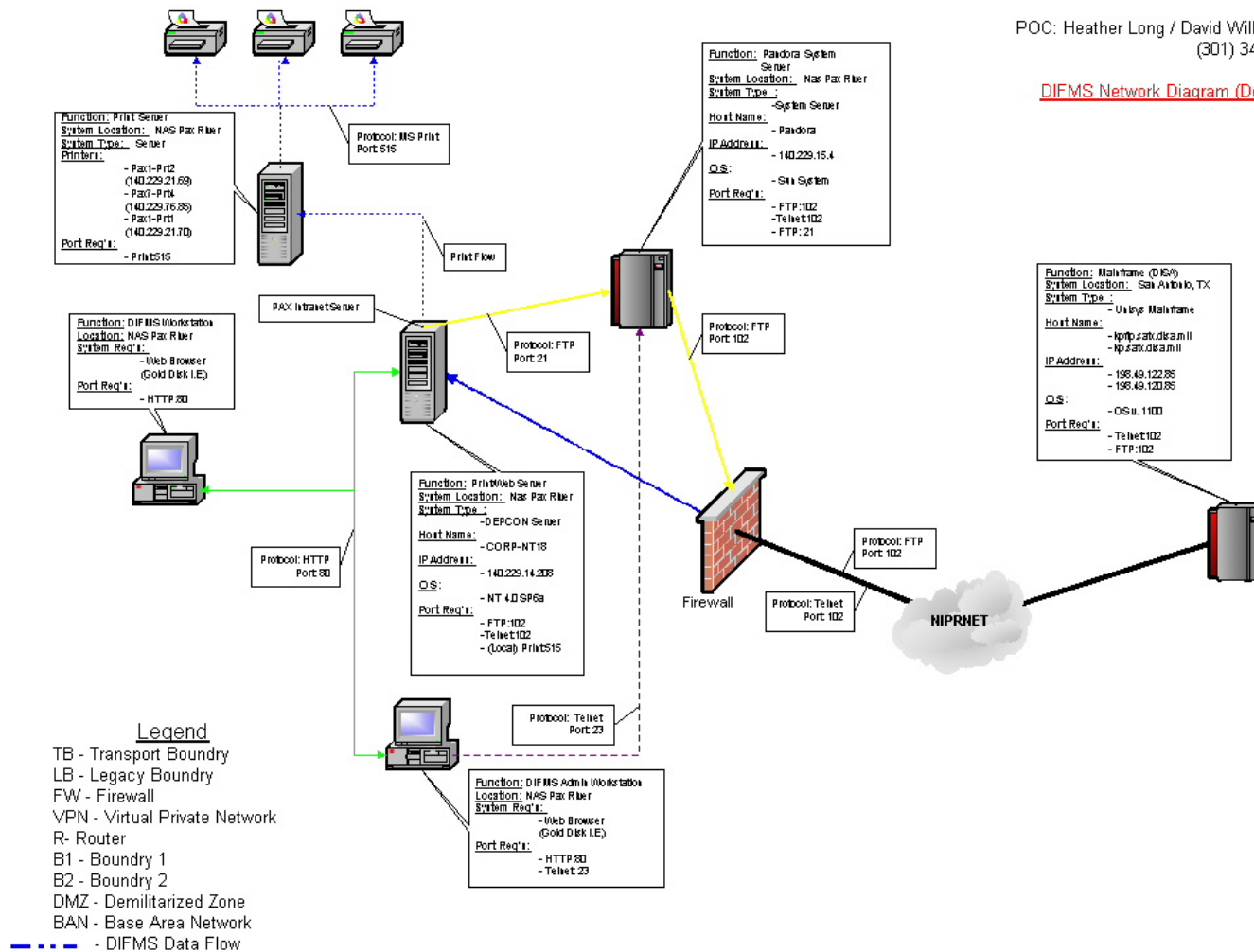
[illegible]

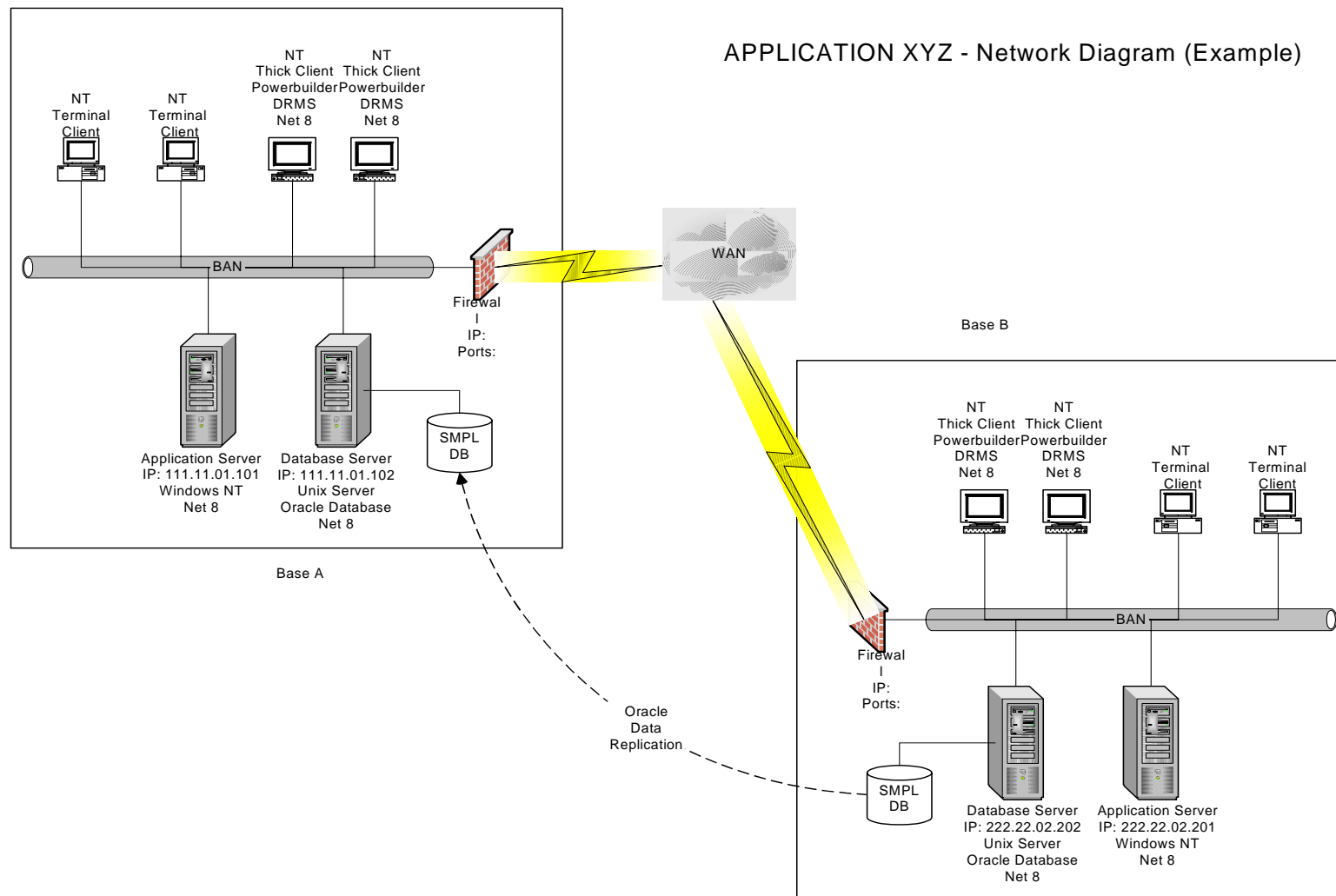
## I4. Example of Systems Architecture Connectivity Diagram



RFS: 2274  
 Defense Industrial Financial Management System (DIFMS)  
 v.00A  
 POC: Heather Long / David Willenborg  
 (301) 342-4621

DIFMS Network Diagram (Detailed)





## **I5. EDS Sherman Street Complex Visitor Request**

The following procedures must be followed for personnel visiting the EDS Sherman Street Complex, San Diego, CA. Visit requests will be mailed or fax'd using the information provided below. Visitor requests must be received by the EDS Security Officer a minimum of the two (2) working days prior to the scheduled visit date. A sample of an EDS authorized visit form is provided. The three methods to obtain access to the EDS Sherman Street Complex are as follows:

### **Active Duty Military and Government Employee**

1. Complete and submit OPNAV 5521/27

### **Contractor in support of SPAWAR**

1. An official internal company security form requesting access to EDS, or
2. Recertification of previously authorized visit request by Government sponsor

### **Contractor working for NMCI**

1. An official internal company security form requesting access to EDS

The following contact information for EDS is provided:

1. Mailing Address

EDS/NMCI  
Visitor Request  
3970 Sherman Street  
San Diego, CA 92110

2. Telephone and Fax  
Security Officer: (619) 817-3720  
Fax Number: (619) 827-3715

## **I6. ARDRA/Pilot Test**

### **Provide ARDRA/Pilot Test Scope, Strategy, and Timeline**

- Define the scope and strategy for testing the software at one or more sites as required.
- Identify test environment
- Perform user/seat mapping
- Test the script and validate installation instructions.
- Establish and publish the timeline of events from beginning to completion of test.

### **Roles and Responsibilities**

- List all personnel directly involved or playing a critical support role in the testing (include them in the communications plan of the RDP).
- List the defined responsibilities assigned to each.

### **Testing Criteria**

- Document the criteria for commencement of testing.
- Provide requisite training to users.
- Evaluate the performance and IA policies of Certified DSL releases.

### **Pilot Installation and Commencement of Testing**

- Summarize the installation work to be done, and what conditions must be met before the application is released to the test group.
- Validate previously documented test scope.
- Document specific features to be tested in a spreadsheet or tabular format.
- Specifically state features NOT be tested.
- Specifically state other items or aspects of the release to be evaluated.
- Validate and update operator interface, user manual usefulness, etc.
- Overall Test Strategy and Timeline.
- Clearly state assumptions related to the testing.

### **Test Descriptions**

- For each major set of tests to be run (such as major functional groups, and performance, stress) describe types of tests to be run.

### **Functional Tests**

- Verification that the software meets its functional/feature requirements.
- Evaluate migration tools used.
- Evaluate Radia applications management performance.

## **Configuration Tests**

- Testing to ensure all functions work under all combinations (hardware configurations, device assignment combinations, other application, etc.).

## **Load and Performance Tests**

- Test to confirm that performance objectives are satisfied; this is separate from previous Beta testing that the Developer performed. Since the Developer is performing this test on a “live” network, it is expected that any other application or function residing on the test group computer retains identical or improved functionality post-installation of the subject test release.
- The NOC pushes the release to test seats set up for ARDRA/Pilot Test. EDS Base Operations verifies that the “Load” occurred, and the application installed properly. Any manual configuration changes needed for the proper installation of a release are **MUST** be noted and evaluated for suitability for use on current and future deployment plans.

## **Stress Tests**

- Testing which attempts to break the system by stressing all of its resources. Recommend that initial tests be performed off hours. If that is not possible, the Developer is required to have appropriate technical personnel available to ascertain which application is questionable.

## **Recovery and Error Handling Tests**

- Testing to confirm that the application recovers from hardware and/or software malfunctions without losing data or control, or that it follows the error handling requirements defined for the application. A “back-out” plan should have been developed in Alpha tests, and it is essential that this “back-out” plan be tested prior bringing the application in a “live” network.

## **Tools and Test Equipment Required**

- Document tools and test equipment required.
- Clearly identify individuals who are expected to provide each.
- Clearly identify who is responsible for the operation of the equipment at each stage.
- Validate migration implementation plan.
- Include printing functions in test script.

## **Problem Recording, Issues Management and Escalation, Rework, and Resolution**

- No changes can be made to the release during ARDRA testing.
- Should the test fail, then the Developer is required to back-out of the release and the release will be sent back to the NMCI Certification process, and be repackaged to the Radia Instance.
- The Developer is to define the mechanism to be used for problem recording and resolution, escalation of issues if necessary, and recording of associated changes required to make to the application.
- Define the process for recording and who is responsible for recording data at each step in the testing.



## **Exit Criteria**

- Document the success criteria to be used to determine adequate system performance.
- Document recommended changes for future releases and include them in release archive.

## **APPENDIX J:    REQUEST TO DEPLOY (RTD)**

This appendix provides the RTD Form and Instruction Guide. The RTD is the vehicle to support the Prioritization and Scheduling processes of releases being deployed into NMCI. The Application Developer or Sponsoring Command is responsible for the completion of the RTD. RTD Instructions Guide will help in completing this form.

J1.	Request to Deploy Form.....	J-2
J2.	Request to Deploy (RTD) Form Instruction Guide .....	J-1

## J1. Request to Deploy Form

NMCI RELEASE SCHEDULING MANAGER (NRSM) ONLY		
Release RTD Number:	Schedule Submission Date: (MM/DD/YYYY)	Required Deployment Date: (MM/DD/YYYY)
<input type="checkbox"/> Approved <input type="checkbox"/> Disapproved	Date of Action: (MM/DD/YYYY)	
Mandatory comment if RTD is disapproved.		

The RTD is the vehicle to support the Prioritization and Scheduling processes of releases being deployed into NMCI. The Application Developer or Sponsoring Command is responsible for the completion of the RTD. Instructions for the completion this form are contained in the RTD Form Instruction Guide.

SECTION 1 – CONTACT INFORMATION			
APPLICATION DEVELOPER – TECHNICAL POC			
1. Full Name:			
2. E-mail Address:			
3. Mailing Address		Street:	
4. City:		5. State:	6. Zip Code:
7. Commercial Telephone Number:			
8. DSN Telephone Number: <b>000-0000</b>			
ACTIVITY/COMMAND			
9. Activity/Command Name:			
10. Mailing Address		Street:	
11. City:		12. State:	13. Zip Code:
14. Activity/Command UIC:			
ACTIVITY COMMAND ALTERNATE POINT OF CONTACT (POC)			
15. Full Name:			
16. Mailing Address		Street:	
17. City:		18. State:	19. Zip Code:
20. E-mail Address:			
21. Commercial Phone Number:			
22. DSN Phone Number: <b>000-0000</b>			
Comments:			
SPONSORING COMMAND REVIEW / APPROVAL			
23. Sponsoring Command Name:			
24. Sponsoring Command UIC:			
25. Command POC Name:			
26. E-mail Address:			
27. Commercial Phone Number:			
28. DSN Phone Number: <b>000-0000</b>			
29. Sponsoring Command/POR Approval: Approved <input type="checkbox"/> Disapproved <input type="checkbox"/> If disapproved provide comment:			

## SECTION 2 – APPLICATION INFORMATION

30. \*\* Application Full Name:

31. Acronym:

32. \*\* Version:

33. CDA RFS number:

34. \*\* DADMS ID number:

35. Type of application: COTS ☐

GOTS ☐

36. What network will this application be deployed to:

NIPRNET ☐

SIPRNET ☐

BOTH ☐

37. Is the application classified?

Yes ☐

No ☐

38. What Service uses this application?

NAVY ☐

USMC ☐

ENTERPRISE ☐

39. Is the release a Joint Application?

Yes ☐

No ☐

40. Purpose, Requirement or Operational use of the application. Describe the Business Process this application supports:

## SECTION 3 – HELP DESK SUPPORT

Help Desk personnel are available to support data-seat-holders around the clock with technical, application, and business questions. Additional information can be obtained at the [NMCI Help Desk](#) web site. Individuals using NMCI seats are instructed to contact the NMCI Help Desk whenever they experience issues with their desktops. Because it is often difficult for a user to distinguish the difference between a desktop issue and an application issue, it is anticipated that many applications issues will be directed to the NMCI Help Desk. When these events occur, the NMCI Help Desk needs to be instructed on how to handle the application issue. This form is intended to capture those requirements.

41. Does this application have its own help desk support? Yes ☐ No ☐

a. If yes, please provide the application help desk information (including point of contact information).

b. If No, in the event of an application issue, please describe how an application issue should be escalated (including point of contact information).

42. What key information is required to be collected by the NMCI Help Desk prior to escalating the issue to the above contacts?

43. Application problem resolution work instructions to the NMCI Help Desk?

## SECTION 4 – APPLICATION IMPLEMENTATION INFORMATION

44. Is this a New Application ☐ or  
Modification/Update/Patch ☐

### Existing Application Information (Upgrades Only)

a. Application Full Name:	
b. Acronym:	c. Version:
d. CDA RFS Number:	
e. If no CDA RFS exists, enter a command RFS:	

45. Provide Technical Description of the Application Release.

46. Does the release have a Required Deployment Date (RDD)? Yes ☐ No ☐  
If yes, enter the RDD (MM/DD/YYYY)

*Every effort will be made to meet the RDD subject to existing test, certification, and deployment resources available. For planning purposes, the release deployment timeline is 90 days (from the media submission date). Emergency deployments for mission critical releases are approved by NNWC/HQMC C4 on a case-by-case basis.*

47. Enter the date the release media will be ready for submission to the lab for certification:  
(MM/DD/YYYY) Media Shipping Number: (If known)

*The release testing, certification, and deployment schedule is based on the media submission date. Failure to submit the media to the test and certification lab on time will significantly impact the deployment of the release.*

48. What is the impact of the release on mission accomplishment? (Select one)

- ☐ High  
☐ Medium  
☐ Low  
☐ None

Rationale for Impact Selected:

49. What is the impact on the mission if the release is deployed later rather than sooner? (Select one)

- ☐ High  
☐ Medium  
☐ Low  
☐ None

Rationale for Impact Selected:

50. Is the release being used to replace an application scheduled for sunset?

Yes ☐ No ☐

If yes, provide name and version of the applications being replaced.

Application name: Version Number: RFS Number:

51. Does the application provide a solution for a quarantined application? Yes ☐ No ☐

If yes, list the quarantined application:

Application Name Version Number: RFS Number:

52. Does the release improve the security of the application? Yes ☐ No ☐ N/A ☐

53. \*\* Select the release plan, which best describes how it will be processed for deployment. (See Chapter 2 of NRDDG)

☐ Planned Annual Release ☐ Planned Point Release ☐ Unplanned Emergency/Urgent Release

*If Unplanned Emergency/Urgent Release is selected, questions a-c **must be** completed. If the Emergency release submission is not approved by NETWARCOM/HQMC C4, the release will be processed as a Planned Point/Annual Release.*

## SECTION 4 – APPLICATION IMPLEMENTATION INFORMATION

	a. Describe the risk(s) the Urgent Release Resolves:
	b. Describe the operational impact if not released:
	c. Describe its impact to current and future users if not released:

54. If this is a mandated release, check the appropriate box below.

<input type="checkbox"/> Safety	<input type="checkbox"/> Department of Defense
<input type="checkbox"/> Fiscal (Changes that effect military, civilian, and contractor pay)	<input type="checkbox"/> Department of Navy
<input type="checkbox"/> Security (Information Assurance Vulnerability Alert (IAVA))	<input type="checkbox"/> Local Commander
<input type="checkbox"/> Operational	<input type="checkbox"/> Major systems
<input type="checkbox"/> Legal (Requirement or Obligation)	<input type="checkbox"/> Minor systems
<input type="checkbox"/> Congressional (Congressional recording requirements/Budgets)	
<input type="checkbox"/> Ongoing war efforts	
<input type="checkbox"/> Treaty with a Sovereign Nation (i.e., Status of Forces Agreement (SOFA))	

## SECTION 5 – APPLICATION BUILD INFORMATION

55. Select the box(s) which effectively describes complexity of the application

Complex	Simple
<input type="checkbox"/> Server	<input type="checkbox"/> Standalone
<input type="checkbox"/> Client/Server	
<input type="checkbox"/> Web based application (client plug-in)	
<input type="checkbox"/> Requires a database to operate (list the database application in block 58)	
<input type="checkbox"/> Requires other dependent software (see block 58)	

56. Are there any special requirements necessary to support this release? Yes ☐ No ☐ If yes, provide information to support special requirements.

57. If this release is a change to an NMCI deployed application, does this release require any components from that previous deployment? Yes ☐ No ☐

If yes, list deployed components (e.g. DLL, INI, CFG, etc.):  
 File name(s):

58. Are there any special requirements, software dependencies, or hardware necessary to support the deployment of the release/application? Yes ☐ No ☐

List software dependencies information:

RFS Number:	Application name:	Version Number:

## SECTION 5 – APPLICATION BUILD INFORMATION

List hardware dependencies information:

RFS Number:	Application name:	Version Number:

Other special requirements:

## **J2. Request to Deploy (RTD) Form Instruction Guide**

Integration of an application release into the NMCI environment requires the completion of a Request to Deploy (RTD) form. The RTD form is the only authorized means to get a patch, modification, fix, upgrade, new (emerging), and quarantined solutions into the NMCI environment. NETWARCOM has approval authority for all application releases submitted for deployment and has established the NMCI Software Configuration Management (NSCM) organization to track, prioritize, and schedule RTD application releases and facilitates deployment of RTD applications into the NMCI environment.

### **Incomplete RTD Information**

An incomplete or improperly completed RTD will not be processed for prioritization and scheduling. It is the responsibility of the Developer/Command to ensure that all instructions are followed and to provide supporting documentation when required. If information is incomplete, NSCM will suspend the RTD and assign a NSCM Claimant CDA Support (CCS) person to contact the Developer and provide assistance with the completion of the RTD form.

### **RTD Submission**

The completed RTD form is submitted electronically to [nmci\\_scm@spawar.navy.mil](mailto:nmci_scm@spawar.navy.mil). Within a few days of submission the Developer, Alternate Point of Contact (POC), and the Sponsoring Developer will receive an email acknowledgement for the receipt of the RTD. As the application progresses from media submission to testing and certification, and deployment phases additional email notifications will be sent to the Developer, Alternate Point of Contact (POC), and Sponsoring Command in order to keep all concerned informed of the application status.

### **RTD Service Support**

If assistance is required for the completion of the RTD form, contact Service Support Monday through Friday during the hours of 0800 to 1600 (Pacific Time) (619) 524-4554 or through email to [nmci\\_scm@spawar.navy.mil](mailto:nmci_scm@spawar.navy.mil)

### **NMCI Release Scheduling Manager (NRSM) Only**

Do not enter information into this section. The NSCM Scheduling Manager will use this section.



## **SECTION 1 – APPLICATION DEVELOPER/ CENTRAL DESIGN ACTIVITY (DEVELOPER) TECHNICAL POINT OF CONTACT (POC) INFORMATION**

If the application is a commercial-off-the-shelf (COTS) application the Technical Point of Contact will be the Vendor. Provide actual email address and not a website address.

If the application is a Government-off-the-shelf (GOTS) application enter information for the developing activity.

If the application is a Program of Record (POR) application enter information for the Program of Record.

### **APPLICATION DEVELOPER – TECHNICAL POC**

1. Full Name: Enter the Developer's full Name (First Name / Middle Initial / Last Name)
2. E-Mail Address: Enter the Developer's E-Mail address (i.e., harry.jones@navy.mil, smithbj@spawar.navy.mil)
- 3-6. Mailing Address: Enter the Developer's mailing address to include street, city, state and zip code. If the mailing address is to a PO Box include PO Box information in the street address line.
7. Commercial Telephone Number: Enter the Developer's commercial telephone number providing the 3 digit area code and the 7 digit phone number (i.e., (555) 555-1234)
8. DSN Telephone Number: (Defense Switch Network) Enter the Developer's 7 digit DSN telephone number.

### **ACTIVITY/COMMAND**

If COTS application, Product Technical Point of Contact will be the Vendor.

If GOTS application, enter the information of the developing activity.

If POR application, enter information for Program of Record.

9. Activity/Command Name: Enter the name of the Developer's Activity/Command (i.e., NAVAIR, COMPACFLT, NETC, NMOC, etc.).
- 10-13. Mailing Address: Enter the activity/command mailing address to include street, city, state and zip code. If the mailing address is to a PO Box include PO Box information in the street address line.
14. Command/Activity Unit Identification Code (UIC): Enter the designated alphanumeric unit identification code (i.e., N00027).

### **ACTIVITY/COMMAND ALTERNATE POINT OF CONTACT (POC)**

If the Application Developer cannot be reached, an alternate point of contact must be provided. The alternate point of contact should be able to answer questions about technical issues concerning the application.

15. Full Name: Enter the Developer's full Name (First Name / Middle Initial / Last Name)
- 16-19. Mailing Address: Enter the POC's mailing address to include street, city, state and zip code. If the mailing address is to a PO Box include PO Box information in the street address line.
20. E-Mail Address: Enter the POC's E-Mail address (i.e., [harry.jones@navy.mil](mailto:harry.jones@navy.mil), [smithbj@spawar.navy.mil](mailto:smithbj@spawar.navy.mil))
21. Commercial Phone Number: Enter the POC's commercial telephone number providing the 3 digit area code and the 7 digit phone number (i.e., (555) 555-1234)
22. DSN Phone Number: (Defense Switch Network) Enter the POC's 7 digit DSN telephone number.

Note: Comment box is provided to place any comments.

## **SPONSORING ECHELON /POR REVIEW/APPROVAL**

The RTD requires a sponsor. This section must be completed by the sponsoring COMMAND before the RTD is submitted for processing.

23. Sponsoring Command Name: Enter the name of the Developer's Activity/Command (i.e., NAVAIR, COMPACFLT, NETC, NMOC, etc.). This is the Command that is being supported by the Developer. Example: A SPAWAR DEVELOPER developing a release for NAVAIR, NAVAIR is the Sponsoring Command.
24. Sponsoring Command UIC: Enter the designated alphanumeric unit identification code (i.e., N00027).
25. Command POC Name: Enter the Full Name (First Name / Middle Initial / Last Name) of the designated POC at the Sponsoring Command for this release.
26. Email Address: Enter the POC's E-Mail address (i.e., [harry.jones@navy.mil](mailto:harry.jones@navy.mil), [smithbj@spawar.navy.mil](mailto:smithbj@spawar.navy.mil))
27. Commercial Phone Number: Enter the POC's commercial telephone number providing the 3 digit area code and the 7 digit phone number (i.e., (555) 555-1234)
28. DSN Phone Number: (Defense Switch Network) Enter the Developer's 7 digit DSN telephone number (000-0000).
29. Sponsoring Command/POR Approval: Select the appropriate box. If "Disapproved" is selected, the Sponsoring Command it is mandatory that a reason for disapproval be stated in the space provided. A disapproved RTD will be sent back to Developer.

## **SECTION 2 – APPLICATION INFORMATION**

30. Application Full Name: Enter the full name of the release, this includes a new release or release that modifies, upgrades, or updates an existing application. It is important to ensure that the application name is the same on the RTD as it is listed in the ISF Tools Database and the DON Application & Database Management System (DADMS). Note: Once the RTD has been

submitted for processing a *change to the application name will require that the submitted RTD be canceled and a new RTD completed with the correct application name.*

31. Acronym: Enter the abbreviated name of the application. It is important to ensure that the acronym is the same on the RTD as it is listed in the ISF Tools Database and the DON Application & Database Management System (DADMS).
32. Version: Enter the version number of the application. It is important to ensure that the application version number is the same on the RTD as it is listed in the ISF Tools Database and the DON Application & Database Management System (DADMS). Note: Once the RTD has been submitted for processing a *change to the version number will require that the submitted RTD be canceled and a new RTD completed with the correct version number.*
33. CDA RFS Number: The CDA RFS number is listed in the ISF Tools Database. If there is no CDA RFS, one must be created in ISF Tools.
34. DADMS ID: All applications entered into the NMCI environment must be approved by the Functional Area Manager (FAM). When an application has been approved the application is listed in the DON Application & Database Management System (DADMS) with an identification number. Enter that number here. DADMS can be accessed at <https://www.dadms.navy.mil/>. If an application is not approved by the FAM, the Developer must complete a waiver application prior to submitting the RTD.
35. Type of Application: If the existing application is a Commercial-Off-the-Shelf application check the “COTS” box. If the existing application is Government-Off-the-Shelf application, check the “GOTS” box.
36. What network will this application be deployed to? Check the box that is appropriate NIPRNET (unclassified), SIPRNET (classified), or Both.
37. Is the application classified? Check Yes or No. If yes is selected the CCS person will contact you with special media submission process.
38. What Service uses this application? Check the box that is appropriate. Navy, US Marine Corp or Enterprise
39. Is the release a Joint Application? Check Yes or No. If yes is selected, the sponsor listed for Line 29 must be a Navy Point of Contact (POC)
40. Purpose, Requirement, or Operational use of the application. Describe the Business Process this application supports.

### SECTION 3 – HELP DESK SUPPORT

41. Does this application have its own help desk support? Check Yes or No.
  - a. If yes, provide the application help desk information and point of contact information
  - b. If no, in the event of an application issue, describe how the issue should be escalated and include the point of contact information.

42. What key information is required to be collected by the NMCI Help Desk prior to escalating the issue to the above point of contacts?

For example key information needed by the application help desk may be to provide the Navy Command, Application, Version Number, and problem description

43. Application problem resolution work instructions to NMCI Help Desk

If an application experiences a problem, provide instructions/coordination protocol(s) to resolve the trouble-call between the application help desk and the NMCI Help Desk.

## SECTION 4 – APPLICATION RELEASE INFORMATION

44. Is this a New Application or Modification/Update/Patch? Check the appropriate box. If the release is a new application check the “New Application” box. If the release is to be modified/updated/patched, check the Modification/Update/Patch” box. If the application is an upgrade complete Existing Application Information #a through #e below. *A change in the answer to this question after the RTD has been submitted will result in the cancellation of the submitted RTD and a new RTD completed with the correct description*
- a. Application full name
  - b. Acronym
  - c. Version
  - d. CDA RFS Number
  - e. If no CDA RFS, enter Command RFS
45. Provide Technical Description of the Application Release. List the primary function of the application, for example, this application is a client server application that is used as a property management tool to track equipment
46. Does the release have a Required Deployment Date? Check the appropriate box. If yes is selected, enter the date the application release needs to be deployed in MM/DD/YYYY format. The RDD date should be a minimum 90 days from the date of media submission for non-emergency deployments and 45 days from the date of media submission for emergency deployments.
47. Enter the date the media will be ready for submission to the Lab for Certification. Enter the date that the media will be submitted to the testing and certification lab in MM/DD/YYYY format. Failure to submit media to the test and certification lab on time will impact the deployment of the application release.
48. What is the impact of the release on mission accomplishment? Check the appropriate box. High, Medium, Low, and None. Except for none all other entries require an explanation for the type of impact selected.
49. What is the impact on the mission if the release is deployed later rather than sooner? Check the appropriate box. High, Medium, Low, and None. Except for none all other entries require an explanation for the type of impact selected.

50. Is the release being used to replace an application scheduled for sunset? Check Yes or No. If yes is selected, provide the application name, version number, and RFS number for the application.
51. Does the release provide a solution for a quarantined application? Check Yes or No. If yes is selected, provide the application name, version number, and RFS number for the application.
52. Does the release increase the security of the application? Check Yes, No, or N/A (non-applicable)
53. Select the release plan, which best describes how it will be processed for deployment. See Chapter 2 of the NRDDG. Planned Annual Release, Planned Point Release, and Unplanned Emergency/Urgent Release. If “Unplanned, Emergency/Urgent Release is selected questions a, b, and c must be completed to support requested deployment plan. *Any change to the type of deployment after the RTD has been submitted will require cancellation of the original submission and a new RTD completed with correct release plan.*
  - a. Describe the risk(s) the Urgent Release Resolves
  - b. Describe the operational impact if not released
  - c. Describe its impact to current and future users if not released

Note: All emergency/urgent application releases must be approved by NETWARCOM. If emergency/urgent deployment is requested, a detailed justification for emergency deployment must be included for NETWARCOM consideration.

54. If this is a mandated release? Check the appropriate box. Safety, Fiscal, Security, Operational, Legal, Congressional, Ongoing war efforts, Treaty with a Sovereign Nation, Department of Defense, Department of Navy, Local Commander, Major systems, or Minor systems.

## SECTION 5 – APPLICATION BUILD INFORMATION

55. Select the box(s) which effectively describes complexity of the application. Complex: Server, Client/Server, Web based application (client plug-in), requires a database to operate, require other dependent software. Simple: Standalone.

Note: A *complex application* is any application that has a separate client side and server side, which require network connectivity to be fully functional. A *simple application* is defined as a standalone application that requires installation on an NMCI workstation only, and has minimal to no dependency on network connectivity to function.

56. Are there any special requirements necessary to support this release? Check Yes or No. If yes is selected, provide information to support special requirements. For example, deployment of the client upgrade needs to be coordinated with a server upgrade.
57. If this release is a change to an NMCI deployed application, does this release require any components from that previous deployment? Check Yes or No. If yes is selected, list deployed components (DLL, INI, CFG, etc.) and File Name(s).

**Are there are any special requirements, software dependencies, or hardware necessary to support the deployment of the release application? Check Yes or No. If yes is selected provide the software and hardware dependencies by RFS Number, Application Name, and Version Number. Include any other special requirements.**

## **APPENDIX K:   ADVANCED PUBLISHER .MSI PACKAGING**



# **NMCI Packaging Standards**

## **Best Practices for MSI**

DRAFT Version 1.0

15 January 2004

---





# **Packaging Standards / Best Practices for MSI**

Final  
Version 1.0  
May 27, 2004  
NMCI.90149.01.F+0.E



## Revision History

The Revision History table below lists in chronological order each minor revision of this document. A minor revision is defined as a set of changes affecting fewer than 30 percent of the pages in the document.

Date	Author	Revision Number	Change(s) Made	Affected Page(s)

Entries in the Revision History table are deleted when a document undergoes a major revision, called a document update. A document update is defined as a set of changes affecting more than 30 percent of the pages in the document. Document updates do not need to be listed in the Revision History table. For more information about Navy Marine Corps Intranet (NMCI) documentation, contact the manager of the Document Management Center (DMC) at [ISFDOCSMailbox@eds.com](mailto:ISFDOCSMailbox@eds.com).

## Document Storage

The EDS NMCI Operations Library assigns identification (ID) numbers for NMCI documents and stores the master Microsoft Word editions as well as the PDF versions. The librarian assigns a document ID number and maintains an audit trail of all document versions. To contact the library, telephone or e-mail the EDS NMCI Operations Librarian (James R. Taylor, 703-742-1940, [ISFOPSLibrary@eds.com](mailto:ISFOPSLibrary@eds.com)).

# Table of Contents

1.	General Developer and Packager Guidelines	1
1.1	Application Architecture	1
1.1.1	Machine and User Components	1
1.1.2	Package Composition	2
1.1.3	Package Materials and Administrative Installation Points	2
2.	MSIEXEC command and appropriate switches	4
3.	Enterprise Packaging Standards and Templates	9
4.	Supporting MSI Upgrades	10
5.	Unattended Enterprise Deployment Guidelines	12
5.1	Run Installation Unattended / Attended	12
5.2	Suppression of Reboot and the Force Reboot Property	12
5.3	Property Overrides	12
6.	Guidelines for Non-MSI Package Re-Authoring	14
7.	References	15

## 2 GENERAL DEVELOPER AND PACKAGER GUIDELINES

The **NMCI Release Development and Deployment Guide** (NRDDG) provides general guidelines for application development. These standards already apply to CDAs; however, to clarify MSI Packaging Standards, the following pertains:

- These general guidelines for application development are provided for reference. Referenced sources for this document are from Microsoft, Novadigm, and Chapter 4 of the NRDDG.
- Successful application deployment depends not only on how applications are packaged and installed, but also on how applications are architected. The general recommendations in this document affect how applications operate when installed, and allow for applications to be successfully deployed in Enterprise environments.

### 2.1 APPLICATION ARCHITECTURE

Applications should be designed to use machine components, such as file and Registry entries, that are identical for all users. User preferences, such as icons, settings, and Registry values, should be stored such that one user does not and cannot affect another user's settings.

Machine components are global settings for the machine shared by all users of the application.

- Machine components affect all users.
- Applications should not require users to have write permission to machine components.
- Machine components should be able to be deployed when no user is logged onto a workstation.
- Machine components include HKEY\_LOCAL\_MACHINE, shortcuts and settings stored in the All Users profile.
- Application files generally are to be found under the "Program Files" directory.
- Applications should avoid using HKEY\_USERS\DEFAULT as a repository for configuration information. Applications running as system services should utilize HKEY\_LOCAL\_MACHINE for settings.

User components are specific to each user of the application. The application should be able to initialize user settings upon first launch either internally to the application or via advertised shortcuts.

- User settings should be stored in the HKEY\_CURRENT\_USER or within the user's profile.
- User settings should support Roaming Profiles.
- A user's preferences should not affect another user's preferences.

#### 2.1.1 Machine and User Components

- The MSI package should support the ability to fully deploy necessary components (machine components) during an unattended installation, even when no user is logged onto the workstation.
- Windows Installer should install user components at the time of application installation if the user is logged onto the workstation or upon first application launch via advertised shortcuts,

which will validate key files and Registry entries to ensure that the user components are initialized before the application is executed. If the user settings do not need to be initialized to a particular customized value, user components could be created by the application when launched.

- The ALLUSERS=1 property should be used to assure proper deployment of advertised shortcuts to the “All Users” profile when applications are to be deployed during an unattended nightly process but available to all users once they logon.
- If an application is expected to be available to only one user, then ALLUSERS=”” will install the application only for the user. Windows Installer may require the user have elevated privileges in order to install the application.

### **2.1.2 Package Composition**

- Use logical directories and root points within the MSI. This allows for the MSI to be portable across configurations.
  - Example: [ProgramFilesFolder] vs. “C:\Program Files” will support users who utilize a second drive partition with the path “D:\Program Files”. For example, applications that need to run on terminal servers may need to support an alternate system drive other than “C:” and should support automatic use of the system drive or logical directory.
- Advertise Registry keys and shortcuts to support self-healing.
- When significant differences exist between a platform or operating system build (image) versions of an application, it is recommended that separate packages be created for deployment to each platform or build. This allows for an automation system to control and limit, on a platform basis, which MSI package is to be deployed.
- Where platform, OS, or image-specific versions of an application only differ by a few components or settings, a single MSI can be created to support the multiple platforms, provided those changes are relatively small in size by comparison.

### **2.1.3 Package Materials and Administrative Installation Points**

In order to efficiently distribute application components across a network, all MSI packages should utilize an Administrative Installation Point (AIP). An AIP allows the application source to be located on a network share or behind a web server. Windows Installer will download only the necessary components based upon the MSI package from the AIP.

- Avoid using multiple MSIs to do what a single MSI could accomplish. Use a single MSI for installing the entire application—however, each MSI should only contain a single “product or application.”
- The MSI should support creation of an Administrative Installation Point (AIP) in order to allow Windows Installer to transfer only necessary data for the installation.
- Packages should be extracted to AIPs in order to minimize network bandwidth utilization during application component downloads for installation and repair. Embedding large CAB files within the MSI or even deploying large CAB files that are external to the MSI is less efficient because unused components will be transferred across the network.

- Limit the size of a single Cabinet file. There is a general CAB file limitation of 65,536 contiguous file resources contained within a single CAB file. If an application requires a larger number of files, multiple CAB files will be required.
- Some packages may need to reference additional files for custom actions or scripts. These additional components should be included within the MSI so they can be managed by the MSI directly on the target system. They should not be required to be standalone components that were not deployed as part of the MSI package. (Do not allow custom scripts or actions to launch in the current user context. They need to stay with the installation user so they have the permissions of the System account).

**NOTE:** It may acceptable for a package to reference an external DLL or file that is not delivered as part of the package but is expected to already be present on the target system. Standards should be developed regarding external files or components and their locations. If the files are not included within the MSI as a managed component, they should not be located within the MSI directory or sub-directory.

- The MSI should support valid short-file names, which can optimize transfers in Enterprise environments. This does not mean that the entire program itself should use short file names. Rather, the MSI should include short-filename mappings where required to support AIP creation. The MSI should be able to create the AIP with valid short file names. This is done by populating the File, Shortcut, and Directory tables with both short and long file names in the format “short|long file name.”

### 3 MSIEXEC COMMAND AND APPROPRIATE SWITCHES

The following table depicts the “msiexec” command and appropriate switches.

The executable program that interprets packages and installs products is Msiexec.exe. Note that Msiexec also sets an error level on return that corresponds to [system error codes](#). The following table describes the command-line options for this program:

Option	Parameters	Meaning
/i	<i>Package ProductCode</i>	Installs or configures a product.
/f	[p o e d c a u m s v] <i>Package ProductCode</i>	Repairs a product. This option ignores any property values entered on the command line. The default argument list for this option is 'pecms'. This option shares the same argument list as the REINSTALLMODE property.  p - Reinstalls only if file is missing. o - Reinstalls if file is missing or an older version is installed. e - Reinstalls if file is missing or an equal or older version is installed. d - Reinstalls if file is missing or a different version is installed. c - Reinstalls if file is missing or the stored checksum does not match the calculated value. Only repairs files that have msidbFileAttributesChecksum in the Attributes column of the File table. a - Forces all files to be reinstalled. u - Rewrites all required user-specific Registry entries. m - Rewrites all required computer-specific Registry entries. s - Overwrites all existing shortcuts. v - Runs from source and recaches the local package. Do not use the v reinstall option for the first installation of an application or feature.
/a	<i>Package</i>	Administrative installation option. Installs a product on the network.
/x	<i>Package ProductCode</i>	Uninstalls a product.
/j	[u m] <i>Package</i> or [u m] <i>Package</i> /t <i>Transform List</i> or [u m] <i>Package</i> /g <i>LanguageID</i>	Advertises a product. This option ignores any property values entered on the command line. u - Advertises to the current user. m - Advertises to all users of machine. g - Language identifier. t - Applies transform to advertised package.

Option	Parameters	Meaning
/L	[i w e a r u c m o p v x + !] <i>Logfile</i>	<p>Specifies path to log file. Flags indicate which information to log.</p> <p>i - Status messages.</p> <p>w - Nonfatal warnings.</p> <p>e - All error messages.</p> <p>a - Start up of actions.</p> <p>r - Action-specific records.</p> <p>u - User requests.</p> <p>c - Initial UI parameters.</p> <p>m - Out-of-memory or fatal exit information.</p> <p>o - Out-of-disk-space messages.</p> <p>p - Terminal properties.</p> <p>v - Verbose output.</p> <p>x - Extra debugging information. Only available on Windows Server 2003.</p> <p>+ - Append to existing file.</p> <p>! - Flush each line to the log.</p> <p>"" - Wildcard, log all information except for the v and x options. To include the v and x options, specify "/!*vx".</p>
/m	<i>filename</i>	<p>Generates an SMS status .mif file. Must be used with either the install (-i), remove (-x), administrative installation (-a), or reinstall (-f) options. The ISMIF32.DLL is installed as part of SMS and must be on the path.</p> <p>The fields of the status mif file are filled with the following information:</p> <p>Manufacturer - Author</p> <p>Product - Revision Number</p> <p>Version - Subject</p> <p>Locale - Template</p> <p>Serial Number - not set</p> <p>Installation - set by ISMIF32.DLL to "DateTime"</p> <p>InstallStatus - "Success" or "Failed"</p> <p>Description - Error messages in the following order: 1) Error messages generated by installer. 2) Resource from Msi.dll if installation could not commence or user exit. 3) System error message file. 4) Formatted message: "Installer error %i", where %i is error returned from Msi.dll.</p>
/p	<i>PatchPackage[;patchPackage2...]</i>	<p>Applies a patch. To apply a patch to an installed administrative image you must combine options as follows:</p>



Option	Parameters	Meaning
		/p <PatchPackage>[:patchPackage2...] /a <Package>
/q	n b r f	<p>Sets user interface level.</p> <p>q , qn - No UI</p> <p>qb - <i>Basic UI</i> . Use qb! to hide the Cancel button.</p> <p>qr - <i>Reduced UI</i> with no modal dialog box displayed at the end of the installation.</p> <p>qf - <i>Full UI</i> and any authored FatalError, UserExit, or Exit modal dialog boxes at the end.</p> <p>qn+ - No UI except for a modal dialog box displayed at the end.</p> <p>qb+ - Basic UI with a modal dialog box displayed at the end. The modal box is not displayed if the user cancels the installation. Use qb+! or qb!+ to hide the Cancel button.</p> <p>qb- - Basic UI with no modal dialog boxes. Please note that /qb+- is not a supported UI level. Use qb-! or qb!- to hide the Cancel button.</p> <p>Note that the ! option is available with Windows Installer version 2.0 and works only with basic UI. It is not valid with full UI.</p>
/? or /h		Displays copyright information for Windows Installer.
/y	module	<p>Calls the system API DllRegisterServer to self-register modules passed in on the command line. For example, msixec /y MY_FILE.DLL.</p> <p>This option is only used for Registry information that cannot be added using the Registry tables of the .msi file.</p>
/z	module	<p>Calls the system API DllUnRegisterServer to unregister modules passed in on the command line. For example, msixec /z MY_FILE.DLL.</p> <p>This option is only used for Registry information that cannot be removed using the Registry tables of the .msi file.</p>
/c		<p>Advertises a new instance of the product. Must be used in conjunction with /t. Available starting with the Windows Installer version shipped with the Windows Server 2003 family and Windows XP SP1.</p>
/n	ProductCode	<p>Specifies a particular instance of the product. Used to identify an instance installed using the multiple instance support through a product code changing transforms. Available starting with the Windows Installer version shipped</p>

Option	Parameters	Meaning
		with the Windows Server 2003 family and Windows XP SP1.

The options /i, /x, /f[p|o|e|d|c|a|u|m|s|v], /j[u|m], /a, /p, /y and /z should not be used together. The one exception to this rule is that patching an administrative installation requires using both /p and /a. The options /t, /c and /g should only be used with /j. The options /l and /q can be used with /i, /x, /f[p|o|e|d|c|a|u|m|s|v], /j[u|m], /a, and /p. The option /n can be used with /i, /f, /x and /p.

To install a product from A:\Example.msi, install the product as follows:

```
msiexec /i A:\Example.msi
```

Only public properties can be modified using the command line. All property names on the command line are interpreted as uppercase but the value retains case sensitivity. If you enter **MyProperty** at a command line, the installer overrides the value of MYPROPERTY and not the value of **MyProperty** in the Property table. For more information, see About Properties.

Steps that NMCI Certification Engineers use to process the Site/Application Developer- Provided MSI:

1. Adhere to the Novadigm Checklist for Publishing Windows Installer Applications via Radia (<http://techsupport.novadigm.com/kb/kb01033.asp>).
2. Full MSI validation using Microsoft's Orca utility (there should be no Errors or Warnings).
3. Create the ACP/AIP (normally placed in the C:\AIP\ApplicationName or C:\AIP\InstanceName subdirectory).

```
msiexec /a application.msi SHORTFILENAME=true /l*v c:
```

4. Install the application from the AIP

```
msiexec /i application.msi /qb ALLUSERS=1 /l*v C:\ACP\ApplicationName\AppInstallMSI.log
msiexec /i application.msi /qr ALLUSERS=1 /l*v C:\ACP\ApplicationName\AppInstallMSI.log
msiexec /i application.msi /qf ALLUSERS=1 /l*v C:\ACP\ApplicationName\AppInstallMSI.log
msiexec /i application.msi /qn ALLUSERS=1 /l*v C:\ACP\ApplicationName\AppInstallMSI.log
```

**NOTE:** The /l\*v C:\ACP\ApplicationName\AppInstallMSI.log enables logging (l) verbose(v) location and filename of the log file.

5. Remove the application using the application.msi from the AIP created in Step 2

```
msiexec /x application.msi /qb
```

To install a product with PROPERTY set to VALUE use the following syntax on the command line. You can put the property anywhere except between an option and its argument.

Correct syntax:

```
msiexec /i A:\Example.msi PROPERTY=VALUE
```

Incorrect syntax:

```
msiexec /i PROPERTY=VALUE A:\Example.msi
```

Property values that are literal strings must be enclosed in quotation marks. Include any white spaces in the string between these marks.

```
msiexec /i A:\Example.msi PROPERTY="Embedded White Space"
```

To clear a public property using the command line, set its value to an empty string.

```
msiexec /i A:\Example.msi PROPERTY=""
```

For sections of text set apart by literal quotation marks, enclose the section with a second pair of quotation marks.

```
msiexec /i A:\Example.msi PROPERTY="Embedded ""Quotes"" White Space"
```

The following is an example of a complicated command line.

```
msiexec /i testdb.msi INSTALLLEVEL=3 /l* msi.log COMPANYNAME="Acme ""Widgets"" and  
""Gizmos.""
```

The following example illustrates advertisement options. Note that switches are not case sensitive.

```
msiexec /JM msisample.msi /T transform.mst /LIME logfile.txt
```

This example shows how to install a new instance of a product to be advertised. This product has been authored to support multiple instance transforms.

```
msiexec /JM msisample.msi /T :instance1.mst;customization.mst /c /LIME logfile.txt
```

This example shows how to patch an instance of a product that has been installed using multiple instance transforms.

```
msiexec /p msipatch.msp;msipatch2.msp /n {00000001-0002-0000-0000-624474736554} /qb
```

When applying patches to a particular product, the /i and /p options cannot be specified in a command line together. In this case, you can apply patches to a product as follows.

```
msiexec /i A:Example.msi PATCH=msipatch.msp;msipatch2.msp /qb
```

**NOTE:** The PATCH property cannot be set in command line, when /p option is used. If the PATCH property is set when the /p option is used, the value of PATCH property is ignored and overwritten.

## 4 ENTERPRISE PACKAGING STANDARDS AND TEMPLATES

- To assure package consistency and productivity, standard packaging processes and templates should be used.
- Templates should incorporate the desired default settings for all packages created within the packaging area - such as permissions, state file filters, library filters, as well as displaying a standard set of bitmaps or banners associated with the packaging area. This will ensure the MSIs created are consistent and visually recognizable as products of a particular packaging area.
- Enterprises should use templates to automate settings for package creation in order to ensure consistency and help eliminate error and omissions in the package creation process.
- Templates should be developed that are consistent with Enterprise standards for directory structure, application locations, security and permissions, etc. that are compatible with the target build environments.

**NOTE:** Standards will vary from Enterprise to Enterprise and may also vary within a single Enterprise depending on the target environments being managed. For example, file locations on Windows 2000 versus Windows XP or file locations on desktops versus laptops. Templates and automation should be used to eliminate variance from the standards.

## 5 SUPPORTING MSI UPGRADES

Proper MSI coding techniques dictate that the MSI should support upgrading. This is the ability to uninstall, reinstall or install over or along side of different versions of the same application. When building an MSI package, an author should be familiar with how the MSI upgrading process works to ensure that their packages are compliant with the best practices for application upgrading. In other words, a package upgrade strategy should be incorporated into the first build of an application package. Windows Installer has package upgrade logic built into the MSI File and Properties tables. Several items must be taken into account to ensure proper upgrading of an application. The following MSI properties help control the upgrade logic:

- **PackageCode:** The PackageCode is actually contained in the MSI file's Summary information, rather than the Property table. It is designed to give each package a unique code. The PackageCode is used like an MD5 hash value to uniquely identify an MSI package.
- **ProductCode:** The ProductCode is a required row of the MSI Property table that uniquely identifies the Product (application) being installed.
- **ProductVersion:** The ProductVersion is also a required row of the MSI Property table. It uniquely identifies the version of the Product being installed in the form Major.Minor.Build.Release. The Windows Installer Engine only uses the first three of these numbers, effectively ignoring the Release number.
- **ProductLanguage:** Another required row of the Property table within the MSI that defines the language for the package using LANGID values (i.e. 1033 for US English).
- **UpgradeCode:** UpgradeCode is an optional row of the Property table that identifies packages that belong in the same Product upgrade group. Though it is an optional row, an UpgradeCode should be entered in preparation for future upgrades.

There are three types of upgrades within Windows Installer: Small, Minor, and Major:

- **Small Upgrade:** The ProductCode and ProductVersion are the same in the older and newer packages. Only the PackageCodes are different. Because the ProductVersion is not changed, there is no way to detect which package contains the newer version of the Product and this type of upgrade is seldom used.
- **Minor Upgrade:** The ProductCode is the same, but the ProductVersion is higher in the newer version. Minor Upgrades will remove existing installations of the Product with a lower version number.
- **Major Upgrade:** With Major Upgrades, the ProductCodes are different and the ProductVersion is higher in the upgrade package, but the UpgradeCodes are the same.

Another concern when upgrading an application is the preservation of customizations made by the user. User customizations can appear within a file or in the Registry.

By default, Windows Installer performs file versioning to determine when a file should be updated with the file in the package. Non-versioned files are considered "User Data"—meaning Windows Installer will compare the Create and Modified dates on the file, and if the Modified date is later than the Create date, the existing file is not replaced, assuming it would remove user customizations in the process.

For customizations maintained in the Registry or INI files, the entry should be set to not replace if it exists. This allows default values to be set if they do not previously exist while preserving user changes to the setting if they do exist.

- Adhere to Microsoft standards for patching and upgrading.  
[http://msdn.microsoft.com/library/en-us/msi/setup/patching\\_and\\_upgrades.asp](http://msdn.microsoft.com/library/en-us/msi/setup/patching_and_upgrades.asp)
- The reference to the Microsoft article on upgrading to a new version of an application can be found in the “Microsoft Platform SDK February 2003 – “Preparing an Application for Future Major Upgrades”  
[http://msdn.microsoft.com/library/en-us/msi/setup/preparing\\_an\\_application\\_for\\_future\\_major\\_upgrades.asp](http://msdn.microsoft.com/library/en-us/msi/setup/preparing_an_application_for_future_major_upgrades.asp)

## 6 UNATTENDED ENTERPRISE DEPLOYMENT GUIDELINES

In order to support Enterprise deployment of applications, an automated system will require that MSI packages provide parameters and options to allow administrators to control the manner in which the packages are installed, updated, and removed from systems.

### 6.1 RUN INSTALLATION UNATTENDED / ATTENDED

Enterprise software management generally requires the ability to perform unattended installation and removal of applications during off-peak hours. Each MSI package should have the ability to run the installation / un-installation un-attended. Unattended installations require the system to be able to provide any configuration information as part of the package installation. If such information is not provided or is user/seat specific, such as the information provided via the user interface during a manual installation, the MSI package should prompt the user during the first launch of the application.

Two areas from the Microsoft Platform SDK are of value:

- **“Command Line Options”** - MSIs should have the ability to run the installation / un-installation quietly. Best Practices would be to use the Microsoft standard MSI command line switches.
- Administrators can set the UI level using the command line option “/q”. A complete list of these command line options can be referenced under the “Using the User Interface” section.

[http://msdn.microsoft.com/library/en-us/msi/setup/command\\_line\\_options.asp](http://msdn.microsoft.com/library/en-us/msi/setup/command_line_options.asp)

[http://msdn.microsoft.com/library/en-us/msi/setup/using\\_the\\_user\\_interface.asp](http://msdn.microsoft.com/library/en-us/msi/setup/using_the_user_interface.asp)

### 6.2 SUPPRESSION OF REBOOT AND THE FORCE REBOOT PROPERTY

The MSI package should support the standard command line options for suppression of the reboots during an installation process. Deferred reboots are generally required to allow an automated distribution system to manage when and how the target nodes are restarted. This may also be required in order for administrators to arrange the sequence an MSI package deployment with other package deployments to the target system.

The MSI package should allow the automation system to manage reboots of the machine when they are required, as other processing may need to occur before or after the MSI package installation.

The package should utilize the MSI REBOOT Property (Force, Suppress, and ReallySuppress), which handles the rebooting of the MSI. If a reboot is required, Windows installer can notify the automation system via return codes 1641 and 3010. The Microsoft Reference for this property is:

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/rebootprompt\\_property.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/rebootprompt_property.asp)

**NOTE:** This is a standard Windows Installer command that can be run with any MSI, so re-packagers do not have an option about utilizing it.

Application packages should not initiate reboots via a custom action. Custom Action reboots can interrupt both the Windows Installer processing as well as an Enterprise automation system.

### 6.3 PROPERTY OVERRIDES

Per the Microsoft Platform SDK, Windows Installer uses three categories of global variables during an installation:

- **Private properties:** The installer uses private properties internally and their values must be authored into the installation database or set to values determined by the operating environment.
- **Public properties:** Public properties can be authored into the installation database in the same way as private properties. In addition, a user or system administrator can change the values of public properties by setting the property on the command line, by applying a transform, or by interacting with an authored user interface. Public property names cannot contain lowercase letters.
- **Restricted public properties:** For security purposes, the author of an installation package can restrict the public properties a user can change.

Not all properties need to be defined in every package. There is a small set of required properties that must be defined in every package. The installer sets the values of properties in a particular order of precedence.

For Enterprise management of any MSI, the settings required by the application should be configured using properties, and any values required during installation should be exposed as public properties or prompted for upon the first launch of the application to facilitate scripted or unattended installation. Examples of properties include application paths, license strings, application host and port settings, etc.



## 7 GUIDELINES FOR NON-MSI PACKAGE RE-AUTHORING

For Enterprise re-packaging of non-MSI application installations into MSI format, several recommendations should be followed in addition to those provided for general application development and packaging guidelines:

- The packaging environment should ensure that packages are built on identical equipment and operating system builds (images) as those in use in production.
- The packaging environment should be configured such that it will be refreshed to a baseline image state prior to each new packaging operation. Ideally, the packaging tool will allow for saving the baseline state as well as the image in order to speed up the scanning process.
- The packaging tool should provide features to automate and adhere to the standards described above. In addition, it should support automation and the use of standardized templates for the enforcement of Enterprise packaging standards for non-MSI package re-authoring as MSIs.
- The packaging tool should provide a wizard-driven process to facilitate a simple and consistent package creation process.
- The packaging tool should automatically populate public and private properties from a variety of different sources such as string substitution, transforms, Registry keys and values, .INI files, environment variables, conditional expressions, and user interface prompts.
- The packaging tool should provide the ability to create a package in the following methods:
  - Component selection mode where the GUI provides an easy way to select just the Registry and file data the administrator wishes to become part of a package.
  - Repackage from an Installation CD where the administrator performs a before and after capture of what the installation deploys to the desktop.
  - Active monitoring of application execution to determine what it does to the desktop as it executes and records the components that are referenced.
- The packaging tool should provide for extensive component filtering to in order to exclude undesired components from the packages. Ideally these filters will be configurable as template settings that can be used across the Enterprise.
- The packaging tool should support the ability to manage file permissions using the Windows Installer Lock Permission Lists in order to implement security permissions for directories, files, and Registry keys.
- The packaging tool should allow an administrator to digitally sign packages to ensure its fidelity.

## 8 REFERENCES

### **NMCI Release Development Deployment Guide (NRDDG)**

<http://www.nmci-isf.com/downloads/ReleaseDevelDeployGuide.zip>

### **Novadigm Radia MSI Guidelines**

<http://techsupport.novadigm.com/kb/kb00609.asp>

### **Microsoft Windows Installer: Benefits and Implementation for System Administrators**

<http://www.microsoft.com/windows2000/techinfo/administration/management/wininstaller.asp>

### **Microsoft's Windows Installer Service Overview**

<http://www.microsoft.com/windows2000/techinfo/howitworks/management/installer.asp>

### **Microsoft ORCA Utility**

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca\\_exe.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/orca_exe.asp)

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/windows\\_installer\\_development\\_tools.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/windows_installer_development_tools.asp)

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/platform\\_sdk\\_components\\_for\\_windows\\_installer\\_developers.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/platform_sdk_components_for_windows_installer_developers.asp)

### **Microsoft Platform SDK - Full Download with Local Install**

<http://www.microsoft.com/msdownload/platformsdk/sdkupdate/psdkredist.htm>

<http://www.microsoft.com/msdownload/platformsdk/sdkupdate/default.htm?p=/msdownload/platformsdk/sdkupdate/psdkredist.htm>

<http://www.microsoft.com/msdownload/platformsdk/sdkupdate/psdk-full.htm>

### **Microsoft: Application Specification for Microsoft Windows 2000 for Desktop Applications**

<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli.asp>

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli\\_appendixa.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli_appendixa.asp)

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli\\_chapter2.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnw2kcli/html/w2kcli_chapter2.asp)

### **Microsoft's "Certified for Windows" program**

<http://www.veritest.com/certification/ms/cfw/>